EXHIBIT 1

Mark C. Mao, CA Bar No. 236165
Sean P. Rodriguez, CA Bar No. 262437
Beko Richardson, CA Bar No. 238027
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899
mmao@bsfllp.com
srodriguez@bsfllp.com
brichardson@bsfllp.com

James Lee (admitted *pro hac vice*)
Rossana Baeza (admitted *pro hac vice*)
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
Fax: (303) 539-1307
jlee@bsfllp.com
rbaeza@bsfllp.com

Amanda K. Bonn, CA Bar No. 270891
SUSMAN GODFREY L.L.P
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA. 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
abonn@susmangodfrey.com

William S. Carmody (admitted *pro hac vice*)
Shawn Rabin (admitted *pro hac vice*)
Steven M. Shepard (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019-6023
Tel.: (212) 336-8330
Fax: (212) 336-8340
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com

John A. Yanchunis (admitted *pro hac vice*)
Ryan J. McGee (admitted *pro hac vice*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CHASOM BROWN, MARIA NGUYEN, WILLIAM BYATT, JEREMY DAVIS, and CHRISTOPHER CASTILLO, individually and on behalf of all other similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 5:20-cv-03664-LHK

FIRST AMENDED COMPLAINT

CLASS ACTION FOR
(1) FEDERAL WIRETAP VIOLATIONS, 18 U.S.C. §§ 2510, *ET. SEQ.*;
(2) INVASION OF PRIVACY ACT VIOLATIONS, CAL. PENAL CODE §§ 631 & 632;
(3) VIOLATIONS OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"),

CAL. PENAL CODE §§ 502 *ET SEQ.*
(4) INVASION OF PRIVACY; AND
(5) INTRUSION UPON SECLUSION.

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Chasom Brown, Maria Nguyen, William Byatt, Jeremy Davis, and Christopher Castillo, individually and on behalf of all others similarly situated, file this First Amended Class Action Complaint against defendant Google LLC ("Google" or "Defendant"), and in support state the following.

INTRODUCTION

"*I want people to know that everything they're doing online is being watched, is being tracked. Every single action you take is carefully monitored and recorded.*"

-Jeff Seibert; Former Head of Consumer Product of Twitter[1]

1. This lawsuit concerns Google's surreptitious interception and collection of personal and sensitive user data while users are in a "private browsing mode." Google does this without disclosure or consent, to profile Plaintiffs and other class members. As a result, from this data, Google reaps billions of dollars in profits each year.

2. Since June 1, 2016 (the "Class Period"), Google has represented that users are "in control of what information [they] share with Google," meaning that they have the power to limit what data Google tracks, collects, and shares with third parties. Google has represented that one way for users to exercise this "control" is by setting their web-browsing software (used to connect to websites) to "private browsing mode."

3. Based on Google's representations, Plaintiffs and Class members reasonably believed that their data would not be collected by Google and that Google would not intercept their communications when they were in "private browsing mode."

4. Google's representations were and are false. Throughout the Class Period, Google unlawfully intercepted users' private browsing communications to collect personal and sensitive information concerning millions of Americans, without disclosure or consent.

5. Google intercepts and collects this data by causing the user's web browsing software to run Google software scripts (bits of code) that replicate and send the data to Google servers in California. These Google software "scripts" do this even if the user is not engaged with any Google

[1] Jeff Orlowski, Davis Coombe, Vickie Curtis, and Larissa Rhodes, *The Social Dilemma*, https://www.netflix.com/title/81254224?s=i&trkid=13747225 (Jan. 2020).

site or functionality and even when the user is in a private browsing mode. These Google software scripts give no notice to the user of Google's data collection methods.

6. Google only recently admitted that it engages in these practices, after Plaintiffs filed their Complaint and in its motion to dismiss. Google previously represented and led users (and regulators) to believe – falsely – that users could limit Google's data collection practices by setting their web-browsing software to private browsing mode.

7. In response to this lawsuit, Google has not disputed that it engages in these interceptions and data collection and instead awkwardly claimed that it fully disclosed what it is doing, and that it therefore has consent to engage in this conduct. Just the opposite is true, as is demonstrated by materials Google itself has cited as the basis for its purported disclosures and consent, as explained below.

8. Google accomplishes its surreptitious interception and data collection through means that include Google Analytics, Google "fingerprinting" techniques, concurrent Google applications and processes on a consumer's device, and Google's Ad Manager. More than 70% of all online publishers (websites) use one or more of these Google services. When a user's web-browsing software accesses one of those websites, hidden Google software "scripts" cause the user's device to send detailed, personal information to Google's servers, including the private browsing communications between the user and the website. This includes the contents of the webpage being requested and the URL viewed.

9. Google's practices infringe upon users' privacy; intentionally deceive consumers; give Google and its employees power to learn intimate details about individuals' lives, interests, and internet usage; and make Google "one stop shopping" for any private, government, or criminal actor who wants to undermine individuals' privacy, security, and freedom.

10. Through its pervasive data tracking business, Google knows who your friends are, what your hobbies are, what you like to eat, what movies you watch, where and when you like to shop, what your favorite vacation destinations are, what your favorite color is and even the most intimate and potentially embarrassing things you browse on the internet—regardless of whether you follow Google's advice to keep your activities "private." Notwithstanding consumers' best efforts,

to keep their activities on the internet private, Google has made itself an unaccountable trove of information so detailed and expansive that George Orwell could never have dreamed it.

THE PARTIES

11. Plaintiffs are Google subscribers whose internet use was tracked by Google during the Class Period, starting on June 1, 2016 and ongoing, while browsing the internet from a browser in a private browsing mode. They bring federal and California state law claims on behalf of other similarly-situated Google users in the United States (the "Classes" defined in Paragraph 192, hereinafter the members of both Classes are referred to as "Class members") arising from Google's knowing and unauthorized interception and tracking of users' internet communications and activity, and knowing and unauthorized invasion of consumer privacy.

12. Plaintiff Mr. Chasom Brown ("Brown") is an adult domiciled in Los Angeles, California. Brown had an active Google account during the entire Class Period.

13. Plaintiff Ms. Maria Nguyen ("Nguyen") is an adult domiciled in Los Angeles, California. Nguyen had an active Google account during the entire Class Period.

14. Plaintiff Mr. William Byatt ("Byatt") is an adult domiciled in Florida. Byatt had an active Google account during the entire Class Period.

15. Plaintiff Mr. Jeremy Davis ("Davis") is an adult domiciled in Arkansas. Davis had an active Google account during the entire Class Period.

16. Plaintiff Mr. Christopher Castillo ("Castillo") is an adult domiciled in California. Castillo had an active Google account during the entire Class Period.

17. Defendant Google is a Delaware limited liability company with a principal place of business at what is officially known as The Googleplex, 1600 Amphitheatre Parkway, Mountain View, California 94043. Google regularly conducts business throughout California and in this judicial district. Google is one of the largest technology companies in the world and conducts product development, search, and advertising operations in this district.

JURISDICTION AND VENUE

18. This Court has personal jurisdiction over Defendant because Google's principal place of business is in California. Additionally, Defendant is subject to specific personal

jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiffs' and Class members' claims occurred in this State, including Google servers in California receiving the intercepted communications and data at issue, and because of how employees of Google in California reuse the communications and data collected.

19. This Court has subject matter jurisdiction over the federal claims in this action, namely the Federal Wiretap Act, 18 U.S.C. § 2511 (the "Wiretap Act") pursuant to 28 U.S.C. § 1331.

20. This Court has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because this is a class action in which the amount in controversy exceeds $5,000,000, and at least one Class member is a citizen of a state other than California or Delaware.

21. This Court also has supplemental jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy as those that give rise to the federal claims

22. Venue is proper in this District because a substantial portion of the events and actions giving rise to the claims in this matter took place in this judicial District. Furthermore, Google is headquartered in this District and subject to personal jurisdiction in this District.

23. Intradistrict Assignment. A substantial part of the events and conduct which give rise to the claims herein occurred in Santa Clara County.

FACTUAL ALLEGATIONS REGARDING GOOGLE

I. Google's History of Privacy Violations & Its Agreement with the FTC

24. Google's violation of consumers' privacy rights is not new – it has been persistent and pervasive for at least a decade.

25. In 2010, the FTC charged that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz." To settle the

matter, the FTC barred Google "from future privacy misrepresentations" and required Google "to implement a comprehensive privacy program."[2]

26. In 2011, Google entered into a consent decree with the FTC (the "Consent Decree"), effective for 20 years, in which the FTC required and Google agreed as follows (emphasis added):

> IT IS ORDERED that [Google], in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:
>
> A. the extent to which [Google] maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information.[3]

27. This requirement applies to the Google conduct at issue in this lawsuit, as the Consent Decree broadly defines "covered information" to include information Google "collects from or about an individual" including a "persistent identifier, such as IP address," and combinations of additional data with the same.

28. Just one year after the Consent Decree was entered, the FTC found that Google had already violated the Consent Decree, by way of Google's misrepresentations regarding what consumer data it would and would not collect with the Safari web browser. In an August 2012 press release, the FTC explained:

> Google Inc. has agreed to pay a record $22.5 million civil penalty to settle Federal Trade Commission charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users, violating an earlier privacy settlement between the company and the FTC.
>
> The settlement is part of the FTC's ongoing efforts make sure companies live up to the privacy promises they make to consumers, and is the largest penalty the agency has ever obtained for a violation of a Commission order. In addition to the civil penalty, the order also requires Google to disable all the tracking cookies it had said it would not place on consumers' computers.

---

[2] https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

[3] https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf.

> "The record setting penalty in this matter sends a clear message to all companies under an FTC privacy order," said Jon Leibowitz, Chairman of the FTC. "No matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place."[4]

29. Since 2012, a number of federal, state, and international regulators have similarly accused Google of violating its promises to consumers on what data it would and would not collect, with Google failing to obtain consent for its conduct.

30. In September 2016, when Google updated its browser app for Apple iOS, Google wrote that users would have "[m]ore control with incognito mode" and "Your searches are your business. That's why we've added the ability to search privately with incognito mode in the Google app for iOS. When you have incognito mode turned on in your settings, your search and browsing history will not be saved."[5] Google made no statements about how users' privacy would actually be limited in these private browsing sessions and avoided for years what it now claims (as a result of this litigation shining the light on its practices): that users never had the privacy they were promised.

31. Similarly, in May 2018, Google modified its privacy policy to state, "[y]ou can use our services in a variety of ways to manage your privacy. . . . You can also choose to browse the web privately using Chrome in Incognito mode."[6]

32. Nonetheless, in 2019, Google and YouTube agreed to pay $170 million to settle allegations by the Federal Trade Commission and the New York Attorney General that YouTube video sharing services illegally collected personal information from children without their parents' consent.

33. Then, in June 2020, France's Highest Administrative Court upheld a 50 million Euro fine against Google based on its failure to provide clear notice and obtain users' valid consent to

---

[4] https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[5] https://www.googblogs.com/the-latest-updates-and-improvements-for-the-google-app-for-ios/. See also, https://search.googleblog.com/index.html.

[6] https://policies.google.com/privacy/archive/20171218-20180525?hl=en-US.

process their personal data for ad personalization purposes.

34. There are ongoing proceedings by the Arizona Attorney General and the Australian Competition and Consumer Commission alleging Google's failure to obtain consent regarding its collection of location data and its decision to combine certain user data.

35. In the Arizona Attorney General action, Google has produced documents establishing "overwhelming" evidence that "Google has known that the user experience they designed misleads and deceives users."

36. Google's employees made numerous admissions in internal communications, recognizing that Google's privacy disclosures are a "mess" with regards to obtaining "consent" for its data collection practices and other issues relevant in this lawsuit. Those documents are heavily redacted by Google, and include for example the following comments and questions by Google employees:

a. "Do users with significant privacy concerns understand what data we are saving?"

b. "[T]ake a look at [redacted by Google] – work in progress, trying to rein in the overall mess that we have with regards to data collection, consent, and storage."

c. "[A] bunch of other stuff that's super messy. And it's a Critical User Journey to make sense out of this mess."

37. Those internal documents are not limited to location data, and unredacted versions of those documents and other internal Google documents will further demonstrate and confirm the lack of consent for the Google conduct at issue in this lawsuit.

38. And in an ongoing Australia proceeding, the Australian Competition & Consumer Commission ("ACCC") alleges that "Google misled Australian consumers to obtain their consent to expand the scope of personal information that Google could collect and combine about

consumers' internet activity, for use by Google, including for targeted advertising."[7] The ACCC contends that Google "misled Australian consumers about what it planned to do with large amounts of their personal information, including internet activity on websites not connected to Google."[8]

II. Google's Privacy Policy, Privacy "Controls," and "Incognito Screen" Each Falsely State that Users Can Prevent Google's Collection By Using "Private Browsing Mode"

39. The public, legislators, and courts have become increasingly aware of online threats to consumer privacy—including threats posed by powerful technology companies like Google that have become household names.

40. To comply with the new laws like the California Consumer Privacy Act (the "CCPA") and Europe's General Data Privacy Regulation (the "GDPR") and to comply with the Consent Decree, Google has repeatedly represented (throughout the Class Period) that users have control over what information is shared with Google and that users can prevent Google from tracking their browsing history and collecting their personal data online.

41. During the Class Period, Plaintiffs and Class members had a reasonable expectation of privacy while they were using a private browser mode. Specifically, Plaintiffs and Class members expected that, when they were using a browser in "private browsing mode," Google (a) would not collect the data described below in Paragraphs 63 through 66, and 78 through 83, and (b) would not thereafter use the data, collected during "private browsing mode," for all of the purposes described below.

42. This expectation of privacy was reasonable because of Google's own statements regarding "private browsing modes" as described below, including the following:

- "***You're in control*** of what information you share with Google . . . ."
- "You can use our services in a variety of ways to manage your privacy . . . across our services, ***you can adjust our privacy settings to control what we collect and***

---

[7] https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data#:~:text=The%20ACCC%20has%20launched%20Federal,Google%2C%20including%20for%20targeted%20advertising.

[8] *Id.*

how your information is used."

- "You can also choose to ***browse the web privately*** using Chrome in Incognito mode."
- "Your search and ad results may be customized using search-related activity even if you're signed out. ***To turn off this kind of search customization, you can search and browse privately***."
- "To browse the web privately, ***you can use private browsing,*** sign out of your account, change your custom results settings, or delete past activity."
- "Your searches are your business. . . . When you have incognito mode turned on in your settings, your search and browsing history ***will not be saved***."

Importantly, Google did not represent in any disclosure to Plaintiffs or Class members that it would continue to intercept, track, and collect communications even when they used a browser while in "private browsing mode."

43. Throughout the Class Period, Google never notified Plaintiffs that Google would intercept users' communications while in a private browsing mode, and that Google was doing so for purposes of creating user profiles or providing targeted advertisings. Google's representations instead misled Plaintiffs and Class members into believing that their communications during private browsing were not intercepted and used to create user profiles or provide targeted advertising.

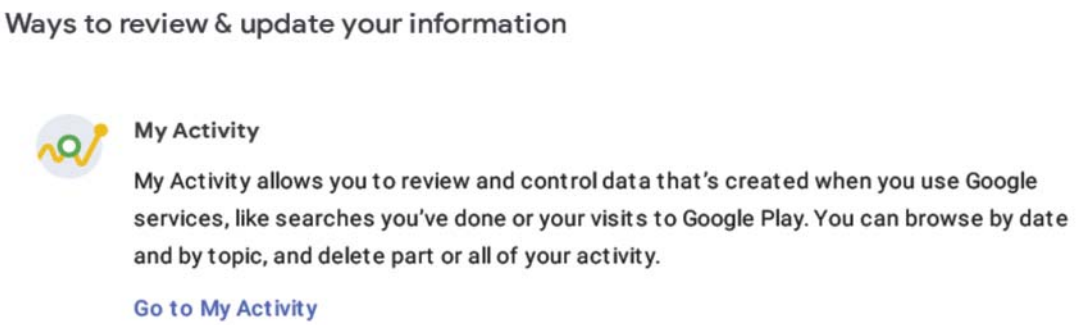
A. Privacy Policy

44. In Google's Privacy Policy (the "Privacy Policy"), throughout the Class Period, Google made numerous representations about how users can "control" the information users share with Google and how users can browse the web anonymously and without their communications with websites being intercepted.

45. Google's Privacy Policy starts by stating in the Introduction section that "you can adjust your privacy settings to control what we collect and how your information is used" and that "[y]ou can choose to browse the web privately using Chrome in Incognito mode":

> on Google or watching YouTube videos. You can also choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

46. The front and center of the "choices" offered to consumers is "Your privacy controls" on the Privacy Policy. Here, Google reiterates, "[y]ou have choices regarding the information we collect and how it's used." On the "My Activity" section of this part of the Privacy



Policy, Google reiterates that "My Activity allows you to review and ***control data that's created when you use Google services,*** like searches you've done."

B. Privacy "Controls"

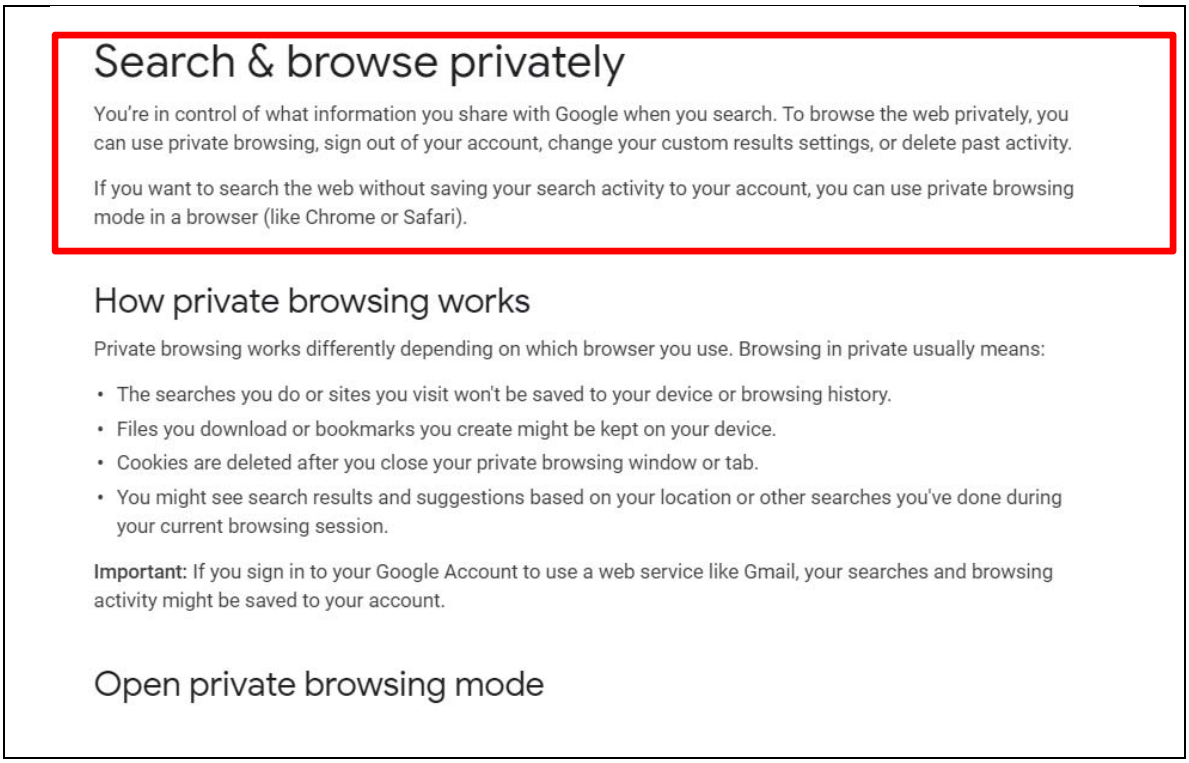
47. Users interested in controlling what Google collects are directed to the "Control Panel" of this same Privacy Policy, where Google assures users that "[t]o browse the web privately, you can use private browsing" and that "[i]f you want to search the web without saving your search activity to your account, you can use private browsing mode in a browser (like Chrome or Safari)."[9] When users click on "Go to My Activity" to control their data, they are presented with the option to "Learn more." When users click on "Learn more," they are taken to a page where they are supposed to be able to "View & control activity in your account." On that page, Google states that you may "[s]top saving activity temporarily. . . . You can search and browse the web privately," embedding a hyperlink to the "Search & Browse Privately" page.[10]

48. On the "Search & Browse Privately" page, Google once again reiterates that the user, not Google, is "in control of what information [a user] . . . share[s] with Google . . . ." Google states simply that consumers enabling "private browsing mode" on their browsers will allow consumers to "browse the web privately":

---

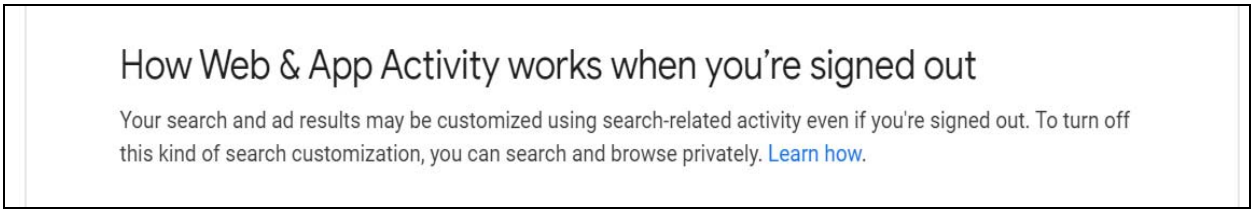
[9] https://support.google.com/websearch/answer/4540094?.

[10] *See* SEARCH & BROWSE PRIVATELY, https://support.google.com/websearch/answer/4540094?hl=en&ref_topic=3036132 (last visited May 29, 2020).



There is nothing on this page about Google Analytics, Google Ad Manager, any other Google data collection tool, or where and which websites online implement such data collection tools.

49. From the "View & control activity in your account" page referenced above, a consumer can also click the link, "See & control your Web & App Activity" on the right-hand side.[11] On that page, Google again represents that searching and browsing in "private browsing mode" will "turn off" any "search customization" "using search-related activity":



50. When users click the "Learn how" link, they are again redirected back to the "Search & Browse Privately" page. In other words, because Google repeatedly touts that users can "control" the information they share with Google and Google constantly refers users back to its recommendations on how users may "browse the web privately," users are left with only one

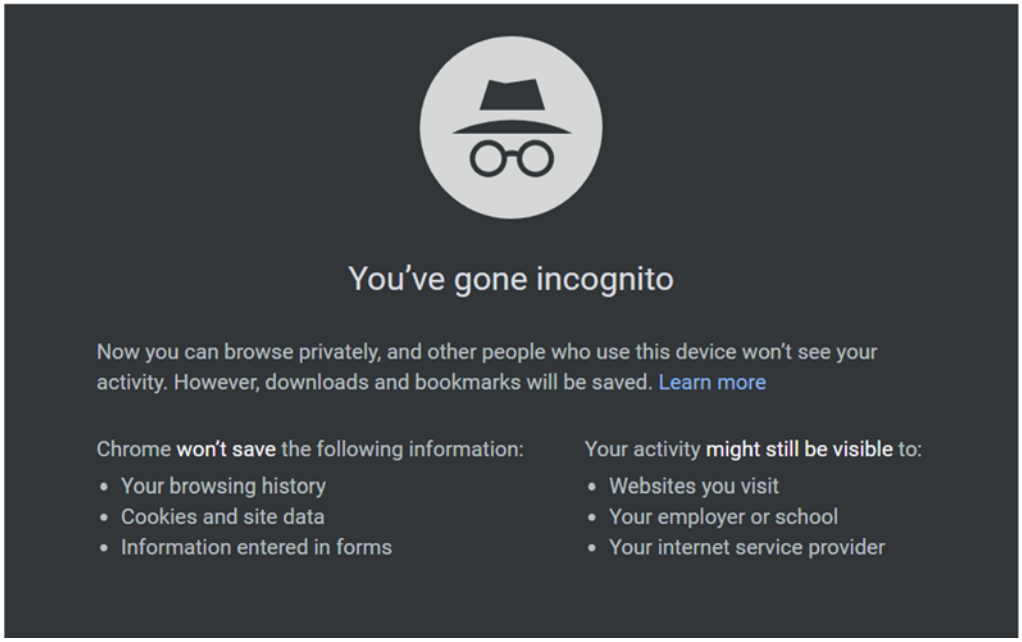
[11] SEE & CONTROL YOUR WEB & APP ACTIVITY, https://support.google.com/websearch/answer/54068?visit_id=637255508625725742210537612 8&hl=en&rd=1 (last visited May 29, 2020).

reasonable impression—if they are searching or browsing the web in "private browsing mode," Google will honor their request to be left alone without further Google tracking.

C. "Incognito Screen"

51. "Incognito" is Google's name for the "private browsing mode" of Google's own web browser software, Google Chrome.

52. Google's first motion to dismiss relies primarily on Google's "Incognito mode" splash screen, which appears when a user opens an Incognito session in Google's Chrome browser (hereinafter the "Incognito Screen"). As Google conceded in its motion, the Incognito Screen appears whenever a user enters Incognito mode:



53. Based on these Google representations, throughout the Class Period, Plaintiffs and Class members reasonably expected that Google would not collect their data while in Incognito mode. They reasonably understood "You've gone incognito" and "Now you can browse privately" to mean they could browse privately, without Google's continued tracking and data collection. Google could have disclosed on this Incognito Screen that Google would track users and collect their data while they were browsing privately, but Google did not do that. Instead, Google included representations meant to assure users that they had "gone incognito" and could "browse privately"

with only limited exceptions, none of which disclosed Google's own tracking and data collection practices while users were in a private browsing mode.

54. Google's Incognito Screen is also deeply misleading for three other reasons. ***First***, Google represents in the Incognito Screen that it "won't save . . . [y]our browsing history . . . cookies and site data[.]" False. In fact, Google's code continues to send the user's browsing history and other data directly to Google's servers during users' private browsing sessions. Google then associates that data with the user's "Google profile" across its services, so that Google can create, update, and monetize detailed profiles on billions of consumers.

55. ***Second***, Google represents in the Incognito Screen that "[n]ow you can browse privately, and other people who use this device won't see your activity." False. In fact, the session is not "private" at all, and "other people who use this device" will still know what preceding users did by way of targeted ads served by Google based on browsing activity that took place during the "private browsing."

56. ***Third***, Google represents in the Incognito Screen that the only entities to whom the user's "activity might still be visible" are "the websites you visit[,] [y]our employer or school[, and] [y]our internet service provider[.]" False. Users' activities are visible to Google, which continues to track users, intercept their communications, and collect their data while they are in Incognito mode and other private browsing modes.

57. What is conspicuously absent from the Incognito Screen – and any other representation by Google – is a disclosure that Google continues to track users while they are in a private browsing mode. Nothing in Google's Privacy Policy or Incognito Screen leads users to believe that during private browsing Google continues to persistently monitor them, and sell their browsing history and communications to other third parties. In fact, when the Privacy Policy and Incognito Screen are read together, the user necessarily reaches the opposite conclusion.

58. There are many other examples of Google representing during the Class Period that users could control what information was shared with Google, including by using a private browsing mode. For example, since May 2018, Google's Privacy Policy has stated: "You can use our services in a variety of ways to manage your privacy. . . . You can also choose to browse the web

privately using Chrome in Incognito mode." In September 2016, Google posted about an update for the Google app for iOS, stating that users would have "[m]ore control with incognito mode" and "Your searches are your business. That's why we've added the ability to search privately with incognito mode in the Google app for iOS. When you have incognito mode turned on in your settings, your search and browsing history will not be saved."

59. Google's representations about how it does not track users under these conditions are completely false, and contrary to the new privacy laws and its 2011 Consent Decree. Not only do consumers (including Plaintiffs and Class members) not know about what Google is doing to collect data on them, they have no meaningful way of avoiding Google's data collection practices, even if they are following Google's instructions to "browse the web privately."

D. Plaintiffs Had a Reasonable Expectation of Privacy

60. Plaintiffs' and Class members' expectation of privacy was reasonable, not only because of Google's various representations, but also because of survey data showing the expectations of Internet users. A number of studies examining the collection of consumers' personal data confirms that the surreptitious taking of personal, confidential, and private information—as Google has done—violates reasonable expectations of privacy that have been established as general social norms. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares a subscriber's personal data. Indeed, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing their data and the same percent believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[12]

[12] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds,* CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

61. Similarly, a study published in the *Harvard Business Review* shows that consumers are largely unaware of how their personal information is used by businesses, with less than 25% of consumers realizing that they share their communication history, IP addresses, and web-surfing history when using a standard web browser.[13] It is also simply common sense that Google should not intercept or collect user communications when users are browsing in "private browsing mode," as these steps demonstrate a clear expectation that communications under these circumstances are intended to be private or confidential.

62. Just as importantly, since 2018, states like California passed the CCPA, which requires that data collection practices be disclosed at or before the actual collection is done.[14] Otherwise, "[a] business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."[15]

III. Google Surreptitiously Intercepts Communications Between Users and Websites And Collects Personal and Sensitive User Data Even When the Users are in "Private Browsing Mode"

A. The Data Secretly Collected

63. Whenever a user (even a user in "private browsing mode," including Plaintiffs and Class members) visits a website that is running Google Analytics or Google Ad Manager, Google's software scripts on the website surreptitiously direct the user's browser to send a secret, separate message to Google's servers in California. This message contains:

a. The "GET request" sent from the user's computer to the website. When an individual internet user visits a web page, his or her browser sends a message called a "GET request" to the webpage's server. The GET request serves two purposes: it first tells the website what information is being requested and then instructs the website to send the information back to

---

[13] Timothy Morey, Theodore Forbath & Allison Shoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

[14] Cal. Civ. Section 1798.100(b). *See also*, Nev. Rev. Stat. Section 603A.340.

[15] *Id.*

the user. The copy of the "GET request," which is sent to Google, enables Google to learn exactly what content the user's browsing software was asking the website to display. The GET request also transmits a referer header containing the URL information of what the user has been viewing and requesting from websites online;

b. The IP address of the user's connection to the internet;[16]

c. Information identifying the browser software that the user is using, including any "fingerprint" data (as described further below, *infra*, at Paragraphs 100-105);

d. Any "User-ID" issued by the website to the user, if available (as described further below, *infra*, at Paragraph 69);

e. Geolocation of the user, if available (as described further below, *infra*, at Paragraphs 105-112); and

f. Information contained in "Google cookies," which were saved by the user's web browser on the user's device at any prior time (as described further below, *infra*, at Paragraphs 70-72).

64. To be clear, the second secret transmission directed by Google, containing both the duplicated message and additional data, is initiated by Google code and concurrent with the communications with the third-party website. This diagram illustrates the process:

//

//

//

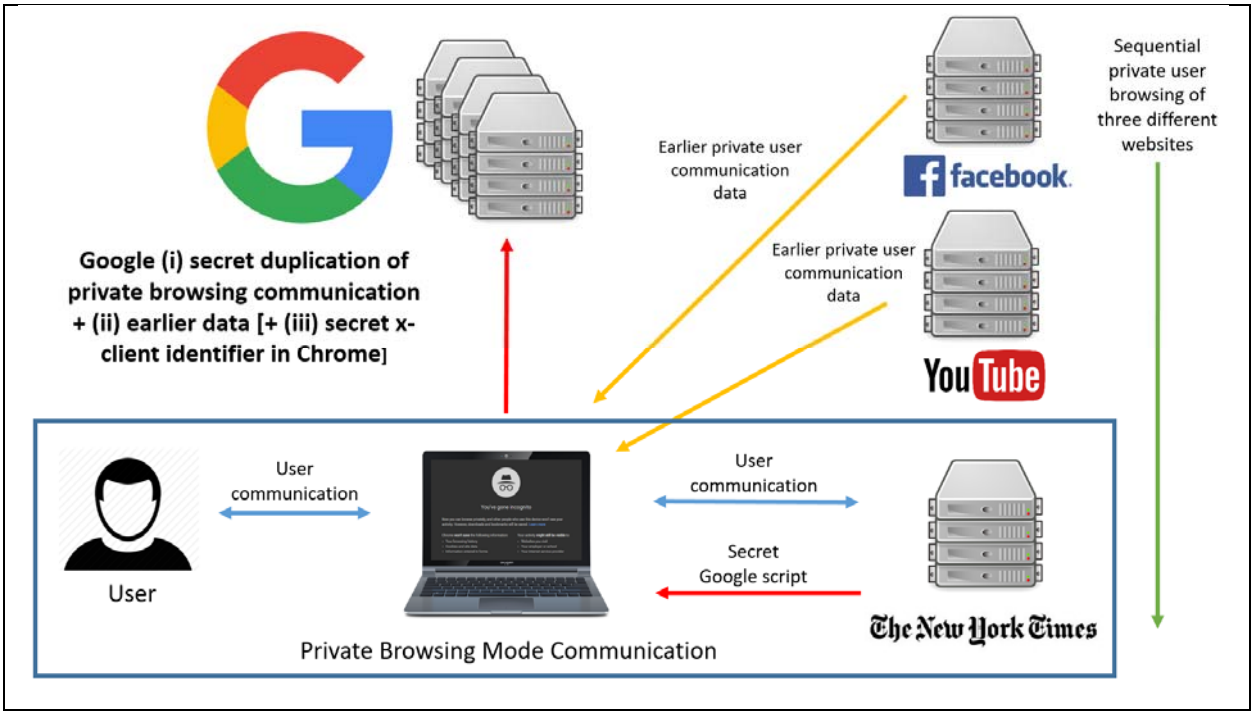
//

//

//

//

[16] IP stands for "Internet Protocol." Each device, when connected to the Internet, is assigned a unique IP address by the Internet Service Provider (ISP) that is providing the internet connection. IP addresses may change over time but often do not. In many cases, an ISP will continue to assign the same IP address to the same device.



65. The above chart illustrates how the user communicates with his or her own web browser in a private browsing mode, for example, by clicking on a link to content the user wishes to view on The New York Times. The user's browser then sends a communication to The New York Times. Because The New York Times is running Google Analytics, Google's embedded Google code, written in Javascript, sends secret instructions back to the user's browser, without alerting the user that this is happening. Google causes the user's browser to secretly duplicate the communication with the website, transmitting it to Google servers in California. Google not only surreptitiously duplicates the data included in the communication with The New York Times but it also includes additional information on the user's prior private browsing histories with Facebook and YouTube, by way of technologies such as cached cookies from prior sessions. Where the user is using Google Chrome, Google also causes to be sent its X-Client-Data Header information if that is available, which uniquely identifies the user.

66. Google does not notify users of this secret Google software code designed to collect user data even while they are in a private browsing mode, which is hidden from users and run without any notice to users of the interception and data collection, which exceeded all contemplated and authorized use of their data. Users also have no way to remove that Google script or to opt-out of its functionality. Google designed the software in a way to render ineffective any barriers users

may wish to use to prevent access to their information, including by browsing in Incognito mode or other private browsing modes. Private browsing modes are supposed to provide users with privacy, as represented by Google, but Google's software by design circumvents those barriers and enables Google to secretly collect user data and profile users.

B. Google Collects Data Using Google Analytics

1. Google Analytics Code

67. Over 70% of online websites and publishers on the internet utilize Google's website visitor-tracking product, "Google Analytics," in addition to other Google advertisement technology products (altogether the "Websites"). Google Analytics is a "freemium" service that Google makes available to websites.[17] Google Analytics provides data analytics and attribution about the origins of a Website's traffic, demographics, frequency, browsing habits on the Website, and other data about visitors. While Google Analytics is used by Websites, it is also essential to Google for its targeted advertisement services, and makes Google Search and its rankings possible by tracking the billions of visits to various Websites every day.

68. To implement Google Analytics, Google requires that Websites embed Google's own custom but blackbox code into their existing webpage code. When a consumer visits a Website, his or her browser communicates a request to the Website's servers to send the computer script to display the Website. The consumer's browser then begins to read Google's custom code along with the Website's own code when loading the Website from the Website's server. Two sets of code are thus automatically run as part of the browser's attempt to load and read the Website pages—the Website's own code, and Google's embedded code. Google's embedded code causes the second and concurrent secret transmission from the user's browser (on the user's computer or other connected device), containing the duplicated message between the user and the Website, to be combined with additional data such as the user's prior browsing history and other Google

[17] Google Analytics is "free" to implement, but the associated data and attribution reports come at a price tag when Websites want more specific information. To obtain more specific and granular data about visitors, Websites must pay a substantial fee, such as by paying for Google's DV360, Ad Hub, or Google Audience products.

trackers, to be sent to Google's servers.

2. User-ID

69. For larger websites and publishers that are able to pay Google's additional fees, Google offers an upgraded feature called "Google Analytics User-ID," which allows Google to map and match the user (including Plaintiffs and Class members) to a specific unique identifier that Google can track across the web. The User-ID feature allows Websites to "generate [their] own unique IDs, consistently assign IDs to users, and include these IDs wherever [the Websites] send data to Analytics." Because of Google's omnipresence on the web, the use of User-IDs can be so powerful that the IDs "identify related actions and devices and connect these seemingly independent data points. That same search on a phone, purchases on a laptop, and re-engagement on a tablet that previously looked like three unrelated actions on unrelated devices can now be understood as one user's interactions with [the website's] business."[18] This User-ID information is even more useful to Google than the individual websites, however. Across millions of websites, Google is able to use its secretly embedded computer scripts and User-IDs to compile what URLs the same users are viewing, even when they are in "private browsing mode," adding all of this information to Google's stockpile of user profiles. In short, with its market power and User-IDs, no one else can track users online like Google.

3. Cookies

70. Google also uses various cookies (hereinafter "Cookies") to supplement Google Analytics' tracking practices. Specifically, Google Analytics contains a script that causes the user's (including Plaintiffs' and Class members') browser to transmit, to Google, information from each of the Google Cookies already existing on the browser's cache. These Cookies typically show, at

[18] *How USER-ID Works*, Google Analytics Help, https://support.google.com/analytics/answer/3123662?hl=en&ref_topic=3123660.

a minimum, the prior websites the user has viewed.[19] These Cookies help enrich Google's profile on the user, which Google uses for its own benefit and profit.

71. Google typically has its Cookies working with Google Analytics coded as "first party cookies,"[20] so that consumers' browsers are tricked into thinking that those Cookies are issued by the Website and not Google. This makes it very difficult for consumers to block Google's Cookies, even if consumers tried to block or clear the cookies issued by "third parties."

72. As discussed earlier, Google's misuse of Cookies on the Safari browser to circumvent user controls was exactly what caused the FTC to fine Google $22.5 million in 2012. The FTC had found that such circumvention of consumer controls and representations were direct violations of the Consent Decree.

4. No Consent

73. Google, as a matter of policy, does not require that Websites disclose how Google Analytics work to consumers (including Plaintiffs and Class members). In fact, as of the date of this First Amended Complaint, Google still only has a "Consent Mode" for Google Analytics, which would help Websites identify whether a particular user (including Plaintiffs and Class members) knows and has consented to their use of Google Analytics and other Google services, in "Beta" or testing mode.[21] "Consent Mode (Beta)" was released for the first time on September 3, 2020, as part of a Google blog entitled, "Measure Conversions While Respecting User Consent Choices."[22]

74. Also, Google does not tell its users which websites implement Google Analytics.

---

[19] A "cookie" is a piece of code that records information regarding the state of the user's system (e.g., username; other login information; items added to a "shopping cart" in an online store) or information regarding the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past). Cookies can also be used to remember pieces of information that the user previously entered into form fields, such as names, addresses, passwords, and payment card numbers. Even in "private browsing mode," Google's "scripts" on websites cause the user's browser to transmit information to Google relating to pre-existing "cookies" on the user's system.

[20] https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage

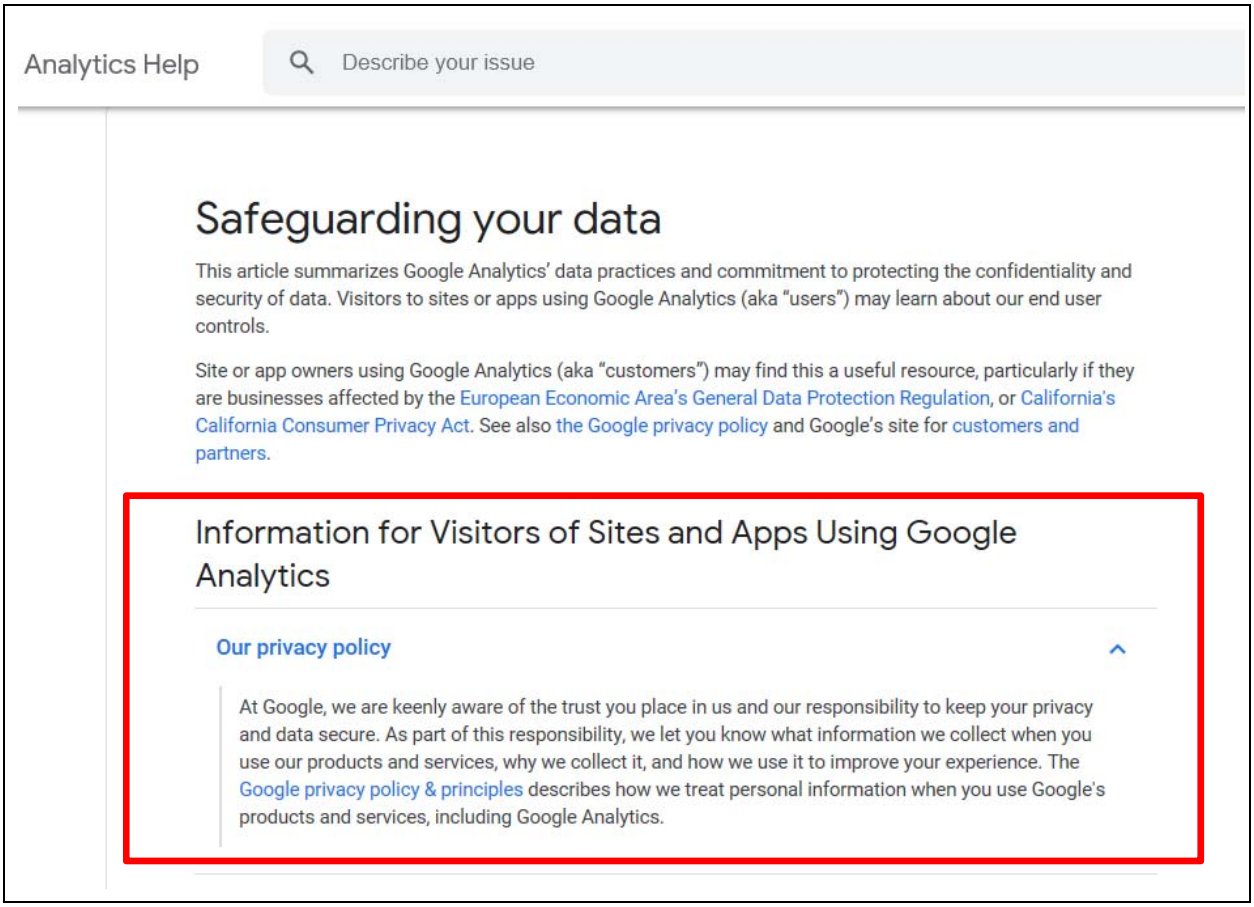
[21] https://support.google.com/analytics/answer/9976101?hl=en.

[22] https://blog.google/products/marketingplatform/360/measure-conversions-while-respecting-user-consent-choices/.

Google starts collecting user data as soon as a page is loading, before a consumer even had the chance to review the page. There is no effective way for users to avoid Google Analytics along with Google's secret interceptions and data collection.

75. Websites implementing Google Analytics do not consent to the Google conduct at issue in this lawsuit, where Google collects consumer data for Google's own purposes and financial benefit while users have enabled "private browsing mode." On information and belief, Google never receives consent from Websites implementing Google Analytics or otherwise that Google may continue to intercept user activity and user data for its own purposes when "private browsing mode" has been enabled.

76. Google's disclosures confirm the lack of consent from Websites to intercept or collect data while users are in "private browsing mode." Google represents to consumers and Websites alike that Google will adhere to its own Privacy Policy as represented, whenever Google Analytics is used. Specifically, Google states on the Analytics Help page for Websites the following, regarding how it follows its own Privacy Policy:



When any Website clicks on the "Google privacy policy & principles" above, they are taken to Google's Privacy Policy homepage at https://policies.google.com/privacy?hl=en, where Google has made assurances to the users such as "you can adjust your privacy settings to control what we collect and how your information is used" and that "[y]ou can choose to browse the web privately using Chrome in Incognito mode." In short, Google has assured Websites that Google Analytics will only be implemented on Websites in such a way that individual users maintain control.

77. Accordingly, Websites implementing Google Analytics have not consented, do not consent and cannot consent to Google's interception and collection of user data for Google's own purposes when users have enabled "private browsing mode" because doing so would violate Google's own Privacy Policy, as well as its assurances that its product complies with privacy laws and the Consent Decree by respecting consumer choice.

C. Google Collects Data Using Ad Manager

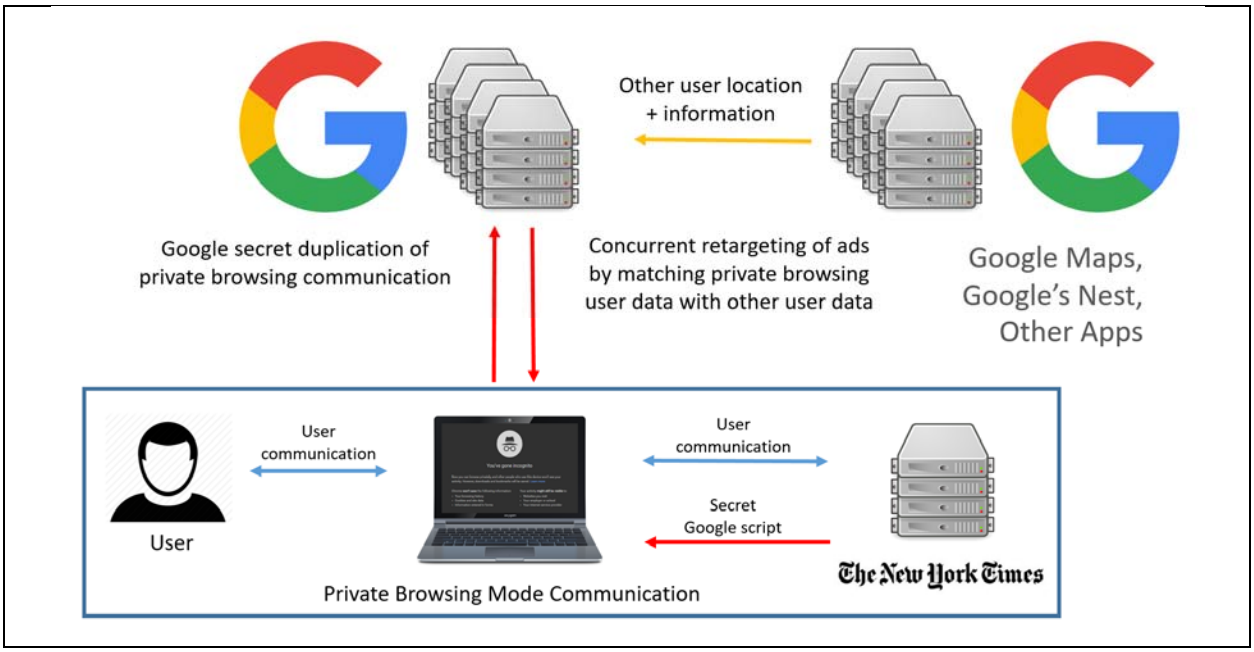
78. In addition to Google Analytics, over 70% of website publishers utilize another Google tracking and advertising product, called "Google Ad Manager" (formerly known as "DoubleClick For Publishers" or "DFP"), which also collects the users' URL viewing history.

79. Like Google Analytics, Google Ad Manager requires Google code to be embedded into the Website's code. When the user's (including Plaintiffs and Class members') browser sends a communication to the website, asking for content to be displayed (i.e., the URL), then the embedded Google code causes the user's browser to display targeted Google advertisements. These targeted ads are displayed along with the Website's actual content. These advertisements are shown to the user on behalf of Google's advertising customers, allowing Google to make money.

80. Google Ad Manager also uses Approved Pixels (*supra*) and Cookies to track users across the internet. Because of the number of Websites that use Google Ad Manager, it is very difficult for consumers (including Plaintiffs and Class members) to avoid its persistence. Like Google Analytics, Google Ad Manager begins collecting information on a user, before the content for the webpage has even fully loaded.

81. To maximize Google's revenue, Google Ad Manager is set up to automatically retarget a user based on information that Google has previously collected, whether this information

is based on a persistent identifier (e.g., Google Analytics User-ID, X-Client-Data Header, *supra*), Google's fingerprinting (e.g., Approved Pixels, *supra*), or geolocation. Thereafter, Google continues to track and target the same user across the internet:



82. In many cases, the intercepted communications provide the "context" for targeted "contextual advertising" for Google, where Google combines the URL the consumer is viewing, with what Google knows about that user (e.g., Google Analytics User-ID, geolocation), to target the consumer in the "context" of his or her web experience. Because of Google's pervasive presence on the internet, its unparalleled reach and its uncanny ability to so target consumers, advertisers are willing to pay a premium for Google's advertisement services.

83. As with Websites implementing Google Analytics, Websites using Ad Manager do not consent to Google collecting data for Google's own purposes while users have enabled "private browsing mode." On information and belief, Google never receives consent from Websites implementing Ad Manager that Google may continue to intercept user activity and user data for its own purposes when "private browsing mode" has been enabled. Indeed, Google represents to consumers and Websites alike that it will adhere to its own Privacy Policy.[23]

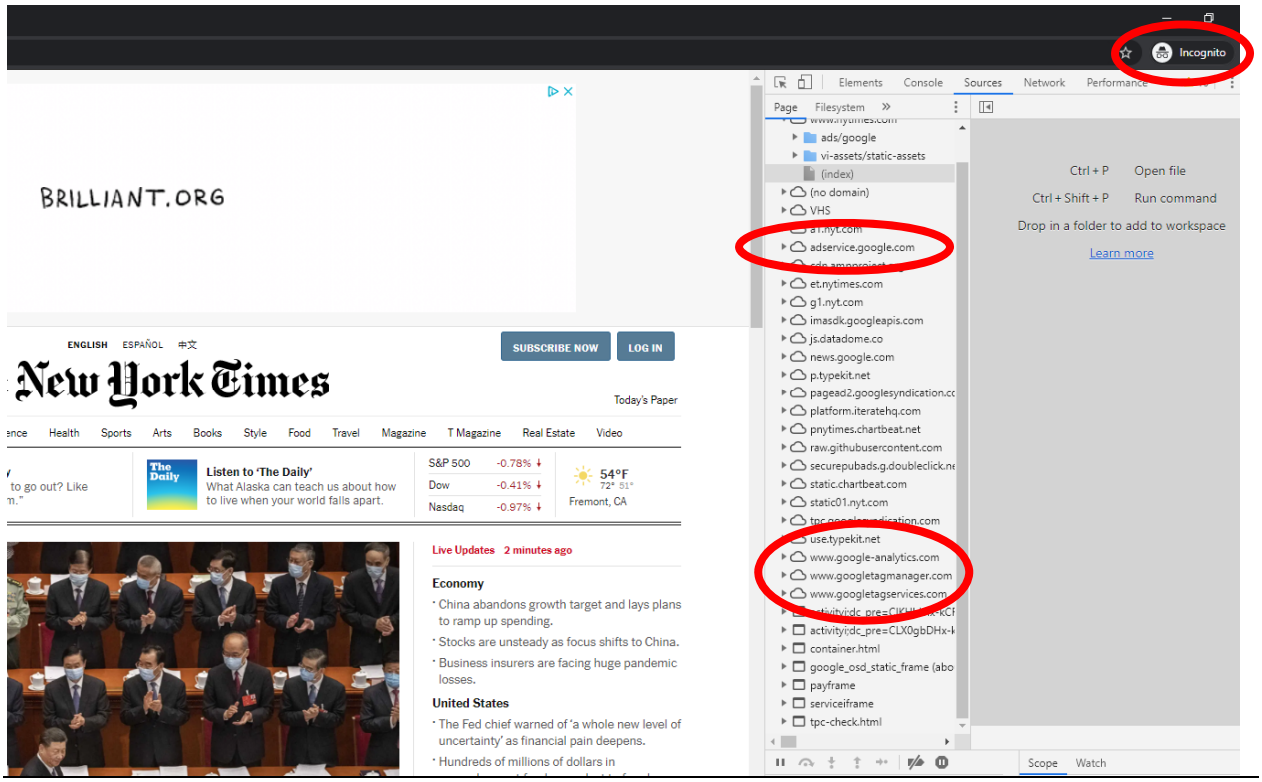
D. Google Collects This Data From Users Even in "Private Browsing Mode"

[23] https://policies.google.com/privacy?hl=en.

84. All of the Google data collection, described above, continues to occur when a user (including Plaintiffs and Class members) enters "private browsing mode" on the user's browser software. Specifically, Google intercepts the communications between the user and the Websites, whenever the user requests any page from the Website, thereby communicating and requesting a specific URL. Google then duplicates this communication and causes it to be sent to its own servers, after pairing the intercepted communications with whatever other data it can collect, so that Google can generate and profit from targeted advertisements.

85. There is no disclosure or consent associated with this Google interception and data collection, as Google designed its software code to run secretly, without disclosure, and render ineffective users' efforts to restrict Google's interception and data collection. Google was never authorized to take and use the information it obtained while users were in a private browsing mode, where users revoked any rights Google might otherwise have had to collect such data.

86. Take, for example, someone who visits *The New York Times* website in private mode with his Google Chrome browser. Even when he is browsing with "private browsing mode" enabled, Google Analytics and Google Ad Manager continue to track his data. This is demonstrated by the following screenshot, which is not presented to the user and accessible only by using developer tools:



87. As described above, Google's secret Javascript code from Google Analytics causes the user to concurrently send to Google not only a duplicated copy of the communications requesting the webpage with the Website but also additional data from the browser, such as Cookies, browser information and the X-Client-Referrer Header if it is available. And Google's Ad Manager not only intercepts the user's communications with the Websites; it concurrently combines the duplicated communications as soon as the user loads a webpage, with data from other Google processes to target the user with advertisements based on the combined information.

88. Thus, even when users are browsing the internet in "private browsing mode," Google continues to track them, profile them and profit from their data whenever they visit a Website that uses Google Analytics or Google Ad Manager. Google collects precisely the type of private, personal information users wish and expect to protect when they have taken these steps to control what information is shared with Google. Google's tracking occurred and continues to occur no matter how sensitive or personal users' online activities are.

IV. Google Creates Profiles On Its Users Using Confidential Information

A. Google's Business Model Requires Extensive And Continual User Data Collection

"This is what every business has always dreamt of; to have a guarantee that if it places an ad, it will be successful. . . . In order to be successful in that business, you have to have great predictions. Great predictions begin with one imperative: you need a lot of data."
-Shoshana Zuboff, PhD; Professor Emeritus, Harvard Business School[24]

89. The core of Google's business model is targeted advertising. In fact, the bulk of Google's hundreds of billions of dollars in revenue annually come from what companies pay Google for targeted advertising,[25] both on Google Search and on various websites and applications that use Google services. The more accurately that Google can track and target consumers, the more advertisers are willing to pay Google's high advertisement fees and services.

90. Allowing consumers (including Plaintiffs and Class members) control over Google's

[24] Jeff Orlowski, Davis Coombe, Vickie Curtis, and Larissa Rhodes, *The Social Dilemma*, https://www.netflix.com/title/81254224?s=i&trkid=13747225 (Jan. 2020).
[25] https://www.investopedia.com/articles/investing/020515/business-google.asp#:~:text=Google%20Ads%20and%20Search%20Advertising,results%20generated%20by%20Google's%20algorithm.

data collections and ad targeting – with an ability to stop Google's data collections and ad targeting, including while in a private browsing mode – is actually against Google's interests and Google's track record with regulators worldwide prove that Google is always tempted to play fast and loose with its obligations and efforts to continue its data collection and ad targeting.

91. Because Google has already collected detailed "profiles" on each user and their devices, Google is able to associate the data (collected from users in private browsing mode) with those users' pre-existing Google "profiles." Doing so improves the "profiles" and allows Google to sell more targeted ads at those users, among many other uses.

B. Google Creates a User Profile on Each Individual

92. Google strives to build "profiles" on each individual (including Plaintiffs and Class members) and each of their devices. These "profiles" contain all the data Google can collect associated with each individual.

93. By tracking, collecting and intercepting users' (including Plaintiffs' and Class members') personal communications indiscriminately—regardless of whether users attempted to avoid such tracking pursuant to Google's instructions—Google has gained a complete, cradle-to-grave profile of users:

a. In many cases, Google is able to associate the data collected from users in "private browsing mode" with specific and unique user profiles through Google Analytics User-ID. Google does this by making use of a combination of the unique identifier of the user it collects from Websites, and Google Cookies that it collects across the internet on the same user;

b. Information collected from Google Cookies, which includes identifying information regarding the user from private browsing sessions and non-private browsing sessions, across multiple sessions;

c. Identifying information regarding the consumer from various Google fingerprinting technologies that uniquely identify the device, such as X-Client-Data Header, GStatic, and Approved Pixels;

d. Geolocation data that Google collects from concurrent Google processes and

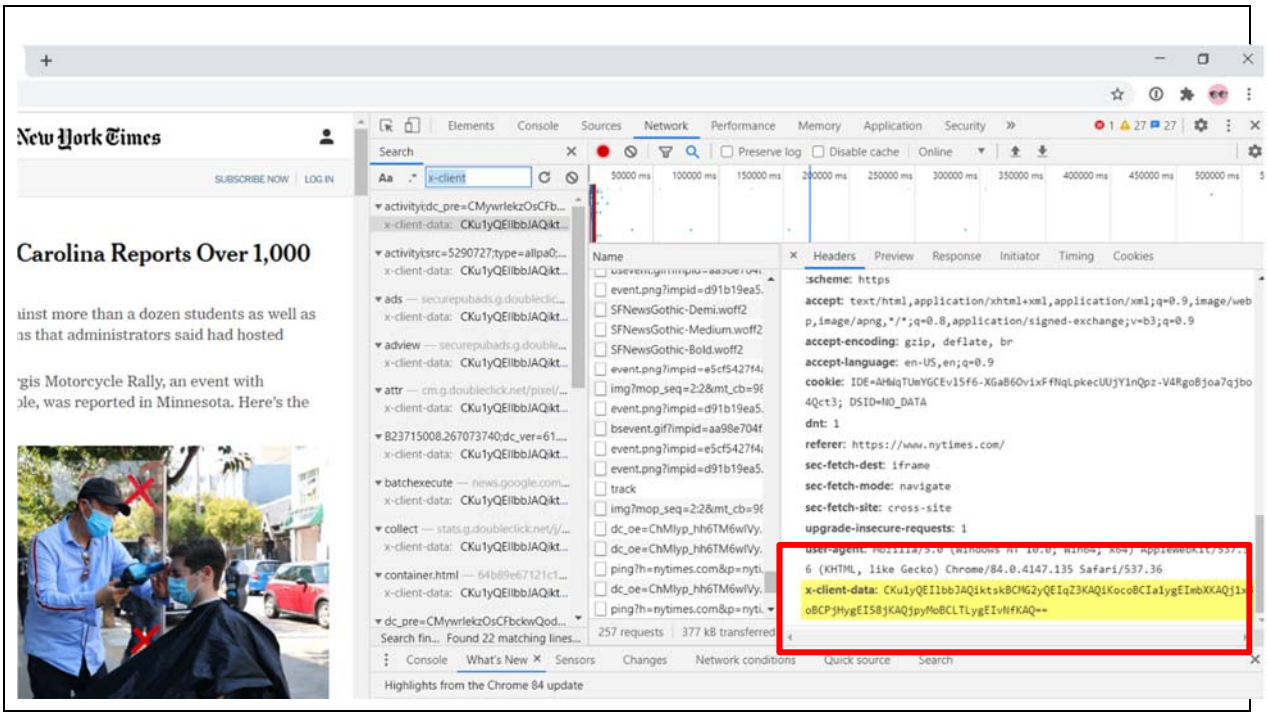
system information, such as from the Android Operating System; and

e. The IP address information, which is transmitted to Google's servers during the private and non-private browsing sessions. Google correlates and aggregates all of this information to create profiles on the consumers.

C. Google Analytics Profiles Are Supplemented by the "X-Client-Data Header"

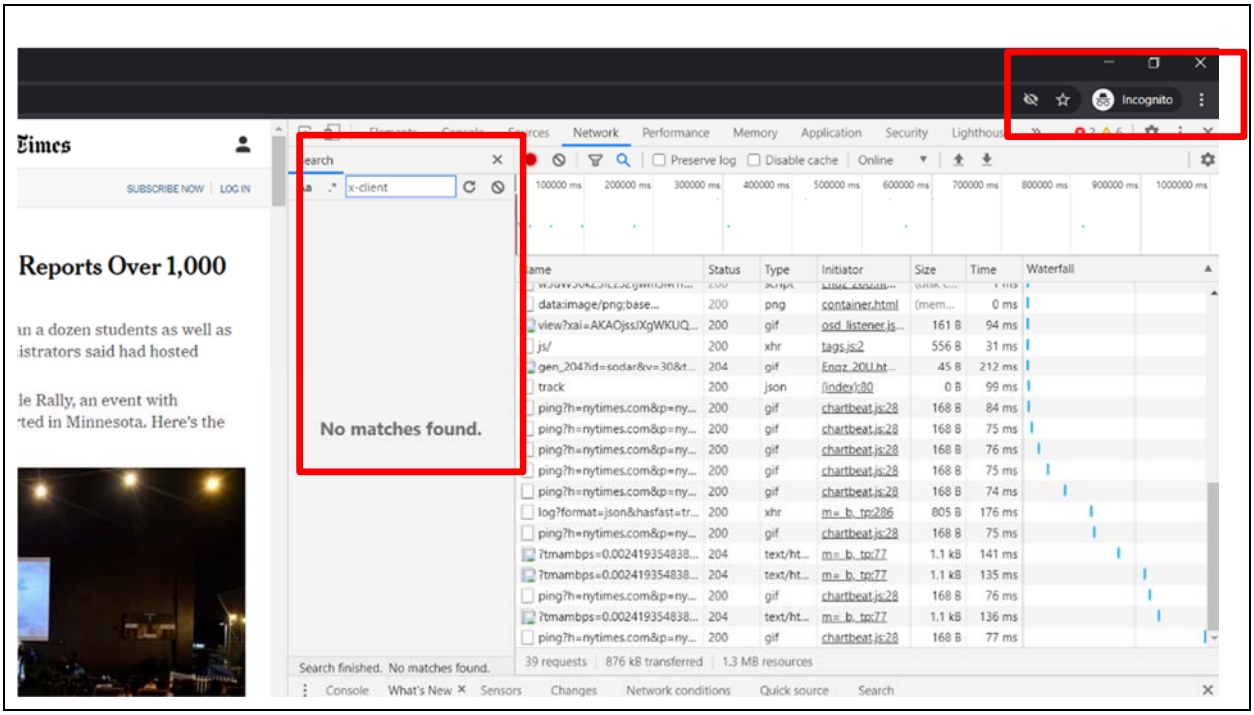
94. Another powerful tool Google uses in building detailed profiles of what may someday be every individual on the planet is the X-Client-Data Header.

95. Google's Chrome browser identifies every device upon the first installation of Chrome with a unique digital string of characters called Google's "X-Client-Data Header," such that Google uniquely identifies the device and user thereafter. Whenever Chrome is used, the Google browser is constantly transmitting this X-Client-Data Header to Google servers. Developer tools confirm this as follows:



96. Through the X-Client-Data Header, Google is able to tell whether a user (including Plaintiffs and Class members) is in Incognito mode or not. The X-Client Data Header is present in

all Chrome-states except when the user is in Incognito mode.[26] Developer tools confirm this as follows:



97. The X-Client-Data Header allows Google to track Chrome users across the web, because it remains unchanged even if users "clear their browser cache" of cookies.[27]

98. Like Cookies, when the X-Client-Data Header is available, Google will concurrently collect this identifier with the duplicated communications it gets from the Websites and browser, to make it near impossible for the consumer to escape Google's surveillance.

99. Google designed the Chrome browser software to track users, which further renders ineffective users' efforts to prevent Google's access to their information and Google's creation of

---

[26] Consistent with its historical behavior, Google actually tried to turn on the X-Client-Data Header for users in March 2020, but was called out by Microsoft engineers on technical forums. https://bugs.chromium.org/p/chromium/issues/detail?id=1060744&q=x-client-data&can=1&mode=grid&start-date=2020-04-23&end-date=2020-05-23&x=Target. Google thereafter called it a "bug," and reverted the browser back to not transmitting the identifier when the user is in Incognito. As Plaintiffs will prove, however, Google was concurrently representing to the press at this time that Google was not so using the X-Client-Data Header in Incognito, when in fact it was. *See, e.g.*, https://www.theregister.co.uk/2020/03/11/google_personally_identifiable_info/.

[27] *See* Thomas Claburn, *Is Chrome Really Secretly Stalking You Across Google Sites Using Per-Install ID Numbers? We Reveal the Truth*, THE REGISTER (Feb. 5, 2020), https://www.theregister.co.uk/2020/02/05/google_chrome_id_numbers/.

detailed user profiles for Google's advertising and profits.

D. Google Identifies You with "Fingerprinting" Techniques

100. Google also builds its profile of users (including Plaintiffs and Class members) by "fingerprinting" techniques. Because every device and application installed has small differences, images, digital pixels, and fonts display differently for every device and application, just ever so slightly. By forcing a consumer to display one of its images, pixels, or fonts, online companies such as Google are able to "fingerprint" their users and consumers across the internet, with or without their permission.

101. For example, a large portion of the Websites also use Google's GStatic, which is a Google-hosted service for fonts, where Google loads the fonts displayed on the Website, instead of the Website's web server. Google sells this service as something that allegedly helps to reduce bandwidth and improve loading time, because Google is hosting the fonts. Plaintiffs are informed and believe and on that basis allege that GStatic is an additional way that Google identifies and tracks consumers, including when consumers are using a private browsing mode.

102. Google also authorizes Websites to place digital pixels ("Google Approved Pixels") embedded within the Websites' code.[28] These pixels are typically created and maintained by "approved third parties" (such as comScore, a data broker registered with California's CCPA data broker registry).

103. Again, when a user's web browser accesses a website containing a Google Approved Pixels, that browser responds to the pixel by generating a unique display. Each user's display is unique because it is generated in part, from certain digital signatures that are unique to each specific device (in combination with the browser software running on the device). By tracking these pixels and the unique resulting displays, Google and its data-broker partners are able to track and "measure" consumers across the web.

---

[28] *See, e.g.*, USE TRACKING PIXELS, https://support.google.com/news/publisher-center/answer/9603438?hl=en (last visited Sept. 20, 2020), describing partnership with comScore.

104. GStatic and Google Approved Pixels enable Google to identify consumers because the way the fonts and pixels are displayed on the browser help to uniquely identify whom the user is. This again is another set of data surreptitiously collected by Google vis-à-vis the consumer's browser which is added to the duplicated communications between the user and Websites, which Google collects concurrent with the user's communications with the Website even when users are in a private browsing mode.

E. Google Identifies You With Your System Data and Geolocation Data

105. Google also collects additional system data and geolocation data from (a) the Android operating system running on users' phones or tablets and (b) Google applications running on phones (e.g., Chrome and Maps), Google Assistant, Google Home, and other Google applications and services.

106. Google collects information for its user profiles (including Plaintiffs and Class members) by making use of (a) the Android operating system, which Google created and makes available for smart phones, and (b) various Google applications that run on mobile devices. In a 2018 white paper entitled "Google Data Collection,"[29] Professor Douglas C. Schmidt of Vanderbilt University concluded that Google's Android operating system, and several of Google's mobile applications, are constantly sending system and location data to Google's servers. Specifically, Professor Schmidt wrote:

> Both Android and Chrome send data to Google even in the absence of any user interaction. Our experiments show that a dormant, stationary Android phone (with Chrome active in the background) communicated location information to Google 340 times during a 24-hour period, or at an average of 14 data communications per hour. In fact, location information constituted 35% of all the data samples sent to Google.

Indeed, now that Google has acquired Nest and merged Nest's data with data obtained via Google Home, Professor Schmidt's analysis regarding Google's ability to identify and track who and where we are is even more persistent and pernicious.

---

[29] Douglas C. Schmidt, *Google Data Collection*, DIGITAL CONTENT NEXT 1 (Aug. 15, 2018), https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.

107. When any user of a Nest or Google Home product is running a Nest or Google Home application, concurrent with Google Assistant, Google is using the data collected from those processes to target users for advertisements. To optimize those advertisements, Google collects the user's geolocation.

108. Because Google Assistant and other Google applications are constantly tracking your geolocation, Google knows exactly who you are, regardless of whether you are in "private browsing mode" on the web, and Google is collecting and profiting from that personal user data.

109. In a *Wired* article regarding Google's privacy practices, Professor Schmidt stated that Google's "business model is to collect as much data about you as possible and cross-correlate it so they can try to link your online persona with your offline persona. This tracking is just absolutely essential to their business. 'Surveillance capitalism' is a perfect phrase for it."[30] By collecting increasing amounts of user data, Google is able to leverage such data to grow its third-party advertising business and profit.

110. Plaintiffs are informed and believe that all of this Google data collection happens even when a consumer is in the web browser's "private browsing mode." Indeed, the Arizona Attorney General recently filed a complaint against Google alleging that it deceptively tracks users based on various sources of location data, overriding consumer privacy controls and preferences.[31]

111. Plaintiffs are informed and believe that Google has contended in private industry conversations and in internal meetings and documents, that such surreptitious data collection is permissible, as it "aggregates the data" after the data has already been intercepted, collected, reviewed, and analyzed by Google. Even if that contention were true, that would not excuse Google's unlawful interceptions of data from users in "private browsing mode."

112. Plaintiffs are informed and believe that Google has also claimed in private industry conversations and in internal meetings and documents that its data collection practices are acceptable and not impermissible interceptions of communications, because Google is "acting on

---

[30] Lily Hay Newman, *The Privacy Battle to Save Google from Itself*, WIRED (Nov. 1, 2018), https://www.wired.com/story/google-privacy-data/.

[31] *See* Complaint, *Arizona v. Google LLC,* Arizona Sup. Ct. Case No. 2020-006219 (May 27, 2020).

behalf of the website(s)", as their vendor. This contention is untrue. As the chart above indicates, Google's secret embedded code causes the user data to be sent directly to Google's servers in California. Google then treats that user data as Google's own property, which Google may use or sell as it pleases. Indeed, for a website to get access to the data that Google has collected using the embedded code running on that website, the website's publisher must pay a premium price to Google.

V. Google Profits from Its Surreptitious Collection of User Data

113. Google's continuous tracking of users is no accident. Google is one of the largest technology companies in the world. Google LLC and its parent Alphabet Inc. have over 1.5 billion active account users, and Alphabet Inc. boasts a net worth exceeding $1 trillion.

114. Google's enormous financial success results from its unparalleled tracking and collection of personal and sensitive user information (including Plaintiffs' and Class members') and selling and brokering of that user information to optimize advertisement services. Over the last five years, virtually all of Google's revenue was attributable to third party advertising and it is continuously driven to find new and creative ways to leverage its access to users' data in order to sustain its phenomenal growth.

115. Google profits from the data it collects – including the user data collected while users are in a private browsing mode – in at least three ways. First, Google associates the confidential communications and data with a user profile or profiles, to enrich Google's ability to charge its customers for advertisement-related services. Second, Google later uses the intercepted confidential communications and user data (in combination with the user's profile) to direct targeted advertisements to consumers (including Plaintiffs and Class members). Third, Google uses the results to improve Google's own algorithms and technology, such as Google Search.

116. The data Google collects contains consumers' personal viewing information. Google collects, reads, analyzes the contents of, and organizes this data based on consumers' prior histories. Google creates "profiles" for each individual user and/or each individual device that accesses the Internet. Google seeks to associate as much information as possible with each profile because, by doing so, Google can profit from Google's ad-targeting services.

117. For example, Plaintiffs are informed and believe and on that basis allege, that Google often demands that websites pay for significant and expensive upgrades (e.g., such as to Google's DV360) in order for the Websites to obtain access to specific visitor information. That Google holds such detailed information regarding visitors hostage is proof that Google collects consumer information on Websites primarily for its own use and profit.

118. Likewise, Google Ad Manager is a service that generates targeted advertisements to be displayed alongside third-party websites' content. The user profiles, which Google creates and maintains using the collected user data, are used by Google's algorithms to select which ads to display through Google.

119. Google is paid for these advertisements by the third-party advertisers. Google is able to demand high prices for these targeted-advertising services because Google is able to use user profiles (including data that Google obtained from users while in "private browsing" mode) to select and display advertisements targeted at those specific profiles.

120. Plaintiffs are informed and believe that Google also benefits by using the data it collects to improve and refine existing Google products, services, and algorithms and also to develop new products, services and algorithms. This collection, usage, or monetization of user data contravenes the steps Plaintiffs and Class members have taken to try to control their information from being tracked or used by Google in any way, for Google's own profits.

121. Google market power in Search is entirely dependent on its ability to track what consumers are doing. The trackers that Google has across the internet not only tell Google where consumers go subsequent to searching on Google Search, the trackers allow Google to track what websites are popular and how often they are visited. By compiling not just consumer profiles, but surveying human behavior across the vast majority of web browser activity, Google is able to create a better and more effective search product as compared to its competitors, by its ability to claim that Google knows how to best rank websites and online properties, because Google can track consumer activity better than anyone else. Google Search would not be nearly as effective of a search tool without Google Analytics as a complement.

122. Google profits from users by acquiring their sensitive and valuable personal information, which includes far more than mere demographic information and volunteered personal information like name, birth date, gender and email address. More importantly, when consumers use Google, Google secretly plants numerous tracking mechanisms on users' computers and web-browsers, which allow Google to track users' browsing histories and correlate them with user, device, and browser IDs, rendering ineffective users' efforts to prevent access to their data.

123. The information Google tracks has and had massive economic value during the Class Period. This value is well understood in the e-commerce industry, and personal information is now viewed as a form of currency.

124. Well before the Class Period, there was a growing consensus that consumers' sensitive and valuable personal information would become the new frontier of financial exploit.

125. Professor Paul M. Schwartz noted in the *Harvard Law Review*:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[32]

126. Likewise, in *The Wall Street Journal*, former fellow at the Open Society Institute (and current principal technologist at the ACLU) Christopher Soghoian noted:

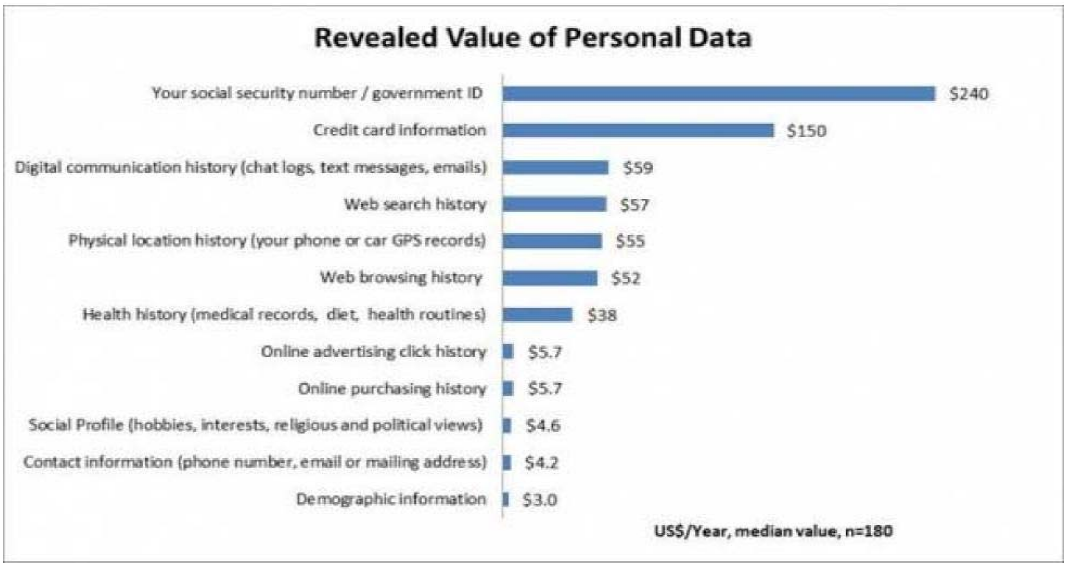
> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.
>
> Although we now regularly trade our most private information for

---

[32] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056–57 (2004).

> access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[33]

127. The cash value of the personal user information unlawfully collected by Google provided during the Class Period can be quantified. For example, in a study authored by Tim Morey, researchers studied the value that 180 internet users placed on keeping personal data secure.[34] Contact information of the sort that Google requires was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year. However, web browsing histories were valued at a much higher rate: $52.00 per year. The chart below summarizes the findings:



128. Similarly, the value of user-correlated internet browsing history can be quantified, because Google itself was willing to pay users for the exact type of communications that Google illegally intercepted from Plaintiffs and other members of the Class during the Class Period. For example, Google Inc. had a panel during the Class Period (and still has one today) called "Google Screenwise Trends" which, according to the internet giant, is designed "to learn more about how everyday people use the Internet."

---

[33] Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011).

[34] Tim Morey, *What's Your Personal Data Worth?*, DESIGN MIND (Jan. 18, 2011), https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html.

129. Upon becoming a panelist, internet users would add a browser extension that shares with Google the sites they visit and how they use them. The panelists consented to Google tracking such information for three months in exchange for one of a number of "gifts," including gift cards to retailers such as Barnes & Noble, Walmart, and Overstock.com.

130. After three months, Google also agreed to pay panelists additional gift cards "for staying with" the panel. These gift cards, mostly valued at exactly $5, demonstrated conclusively that internet industry participants understood the enormous value in internet users' browsing habits. Google now pays Screenwise panelists up to $3 *per week* to be tracked.

131. As demonstrated above, user-correlated URLs have monetary value. They also have non-monetary, privacy value. For example, in a recent study by the Pew Research Center, 93% of Americans said it was "important" for them to be "in control of who can get information" about them. Seventy-four percent said it was "very important." Eighty-seven percent of Americans said it was "important" for them not to have someone watch or listen to them without their permission. Sixty-seven percent said it was "very important." And 90% of Americans said it was "important" that they be able to "control[] what information is collected about [them]." Sixty-five percent said it was very important.

132. Likewise, in a 2011 Harris Poll study, 76% of Americans agreed that "online companies, such as Google or Facebook, control too much of our personal information and know too much about our browsing habits."

133. Consumers' sensitive and valuable personal information increased as a commodity, where Google itself began paying users specifically for their browsing data.[35] As early as 2012 Google publicly admitted it utilized consumers' browsing data, paired with other sensitive and valuable personal information, to achieve what it called "nowcasting," or "contemporaneous

[35] Jack Marshall, *Google Pays Users for Browsing Data*, DigiDay (Feb. 10, 2012), https://digiday.com/media/google-pays-users-for-browsing-data/

forecasting," which Google's Chief Economist Hal Varian equated to the ability to predict what is happening as it occurs.[36]

134. As the thirst grew for sensitive, personal information,[37] it became readily apparent that the world's most valuable resource was no longer oil, but instead consumers' data in the form of their sensitive, personal information.[38]

135. During the Class Period, a number of platforms have appeared where consumers can and do directly monetize their own data, and prevent tech companies from targeting them absent their express consent:

a. Brave's web browser, for example, will pay users to watch online targeted ads, while blocking out everything else.[39]

b. Loginhood states that it "lets individuals earn rewards for their data and provides website owners with privacy tools for site visitors to control their data sharing," via a "consent manager" that blocks ads and tracking on

---

[36] K.N.C., *Questioning the searches*, The Economist (June 13, 2012), https://www.economist.com/schumpeter/2012/06/13/questioning-the-searchers

[37] *Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Paper No. 220 at 7 (Apr. 2, 2013), http://dx.doi.org/10.1787/5k486qtxldmq-en; *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD, at 319 (Oct. 13, 2013), https://www.oecd.org/sti/inno/newsourcesofgrowthknowledge-basedcapital.htm; Pauline Glickman and Nicolas Glady, *What's the Value of Your Data?* TechCrunch (Oct. 13, 2015) https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/; Paul Lewis and Paul Hilder, *Former Cambridge Analytica exec says she wants lies to stop*, The Guardian (March 23, 2018) https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies; Shoshanna Zuboff, The Age of Surveillance Capitalism 166 (2019).

[38] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[39] Get Paid to Watch Ads in the Brave Web Browser, at: https://lifehacker.com/get-paid-to-watch-ads-in-the-brave-web-browser-1834332279#:~:text=Brave%2C%20a%20chromium-based%20web%20browser%20that%20boasts%20an,a%20more%20thoughtful%20way%20than%20we%E2%80%99re%20accustomed%20to (Lifehacker, April 26, 2019) ("The model is entirely opt-in, meaning that ads will be disable by default. The ads you view will be converted into Brave's cryptocurrency, Basic Attention Tokens (BAT), paid out to your Brave wallet monthly").

browsers as a plugin.[40]

c. Ex-presidential candidate Andrew Yang's "Data Dividend Project" aims to help consumers, "[t]ake control of your personal data. If companies are profiting from it, you should get paid for it."[41]

d. Killi is a new data exchange platform that allows you to own and earn from your data.[42]

e. Similarly, BIGtoken "is a platform to own and earn from your data. You can use the BIGtoken application to manage your digital data and identity and earn rewards when your data is purchased."[43]

f. The Nielsen Company, famous for tracking the behavior of television viewers' habits, has extended their reach to computers and mobile devices through Nielsen Computer and Mobile Panel. By installing the application on your computer, phone, tablet, e-reader, or other mobile device, Nielsen tracks your activity, enters you into sweepstakes with monetary benefits, and earn points worth up to $50 per month.[44]

---

[40] https://loginhood.io/. See also, https://loginhood.io/product/chrome-extension ("[s]tart earning rewards for sharing data – and block others that have been spying on you. Win-win.").

[41] How Does It Work, at: https://www.datadividendproject.com/ ("Get Your Data Dividend…We'll send you $$$ as we negotiate with companies to compensate you for using your personal data.").

[42] https://killi.io/earn/.

[43] https://bigtoken.com/faq#general_0 ("Third-party applications and sites access BIGtoken to learn more about their consumers and earn revenue from data sales made through their platforms. Our BIG promise: all data acquisition is secure and transparent, with consumers made fully aware of how their data is used and who has access to it.").

[44] Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, Best Wallet Hacks (June 10, 2020), https://wallethacks.com/apps-for-selling-your-data/.

136. Technology companies recognize the monetary value of users' sensitive, personal information, insofar as they encourage users to install applications explicitly for the purpose of selling that information to technology companies in exchange for monetary benefits.[45]

137. The CCPA recognizes that consumers' personal data is a property right. Not only does the CCPA prohibit covered businesses from discriminating against consumers that opt-out of data collection, the CCPA also expressly provides that: "[a] business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information." Cal. Civ. Code § 1798.125(b)(1). The CCPA provides that, "[a] business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature." Cal. Civ. Code § 1798.125(b)(4).

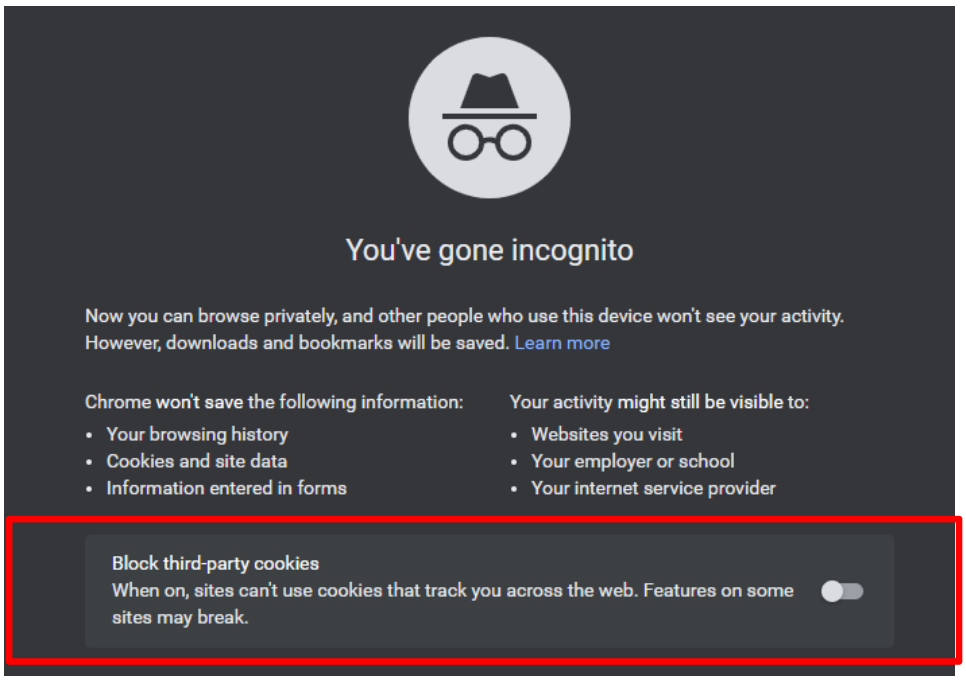
138. Through its false representations and unlawful data collection, Google is unjustly enriching itself at the cost of consumer choice, when the consumer would otherwise have the ability to choose how they would monetize their own data.

VI. Google's Recent About-Face

139. Google has already acknowledged the inappropriateness of its tracking practices in private browsing mode. ***First***, after Plaintiffs filed the instant lawsuit, Google changed its own Incognito Screen to add an additional option of "block[ing] third-party cookies." Google's disclosure is still unclear as to whether the term 'third party cookies' encompasses Google's own 'Doubleclick' cookies and, once again, leaves a misleading impression about Google's own interception and collection of user data. Because Google used its Doubleclick cookies to track users across websites, including when users are in Incognito or some other private browsing mode, Google was able to identify and track users even when they were in such private browser modes:

---

[45] Kari Paul, *Google launches app that will pay users for their data*, The Guardian (June 11, 2019), https://www.theguardian.com/technology/2019/jun/11/facebook-user-data-app-privacy-study; Saheli Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of data*, CNBC (Jan. 30, 2019), https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html; Jay Peters, *Facebook will now pay you for your voice recordings*, The Verge (Feb. 20, 2020), https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounnunciations-app.



Notably, Google provides no explanation of what "third-party cookies" Google is referring to, or that Google may in fact be talking about itself, where Google had been intercepting the user's communications in Incognito for years.

140. ***Second,*** after Plaintiffs filed the instant lawsuit, Google began testing a "Consent Mode (Beta)" for Google Analytics, where Websites for the first time will be required to indicate to Google whether the users agreed to be tracked by Google Analytics and Ad Manager, before "the associated [computer code] tags will function normally" for those products:[46]

//

//

//

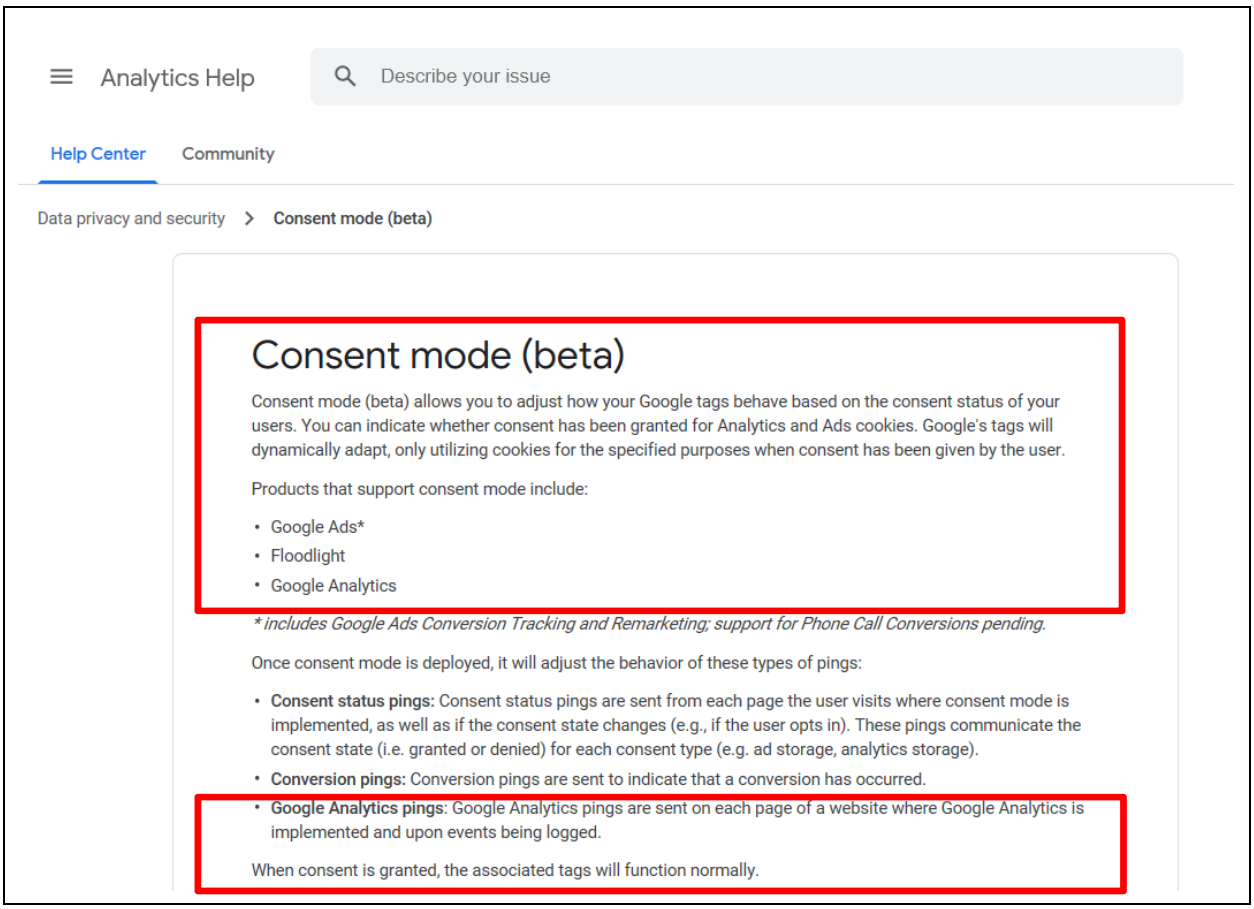
//

//

//

//

[46] https://support.google.com/analytics/answer/9976101?hl=en.



141. Google's release of such functionalities for testing is proof that Google did not previously implement sufficient user controls to ensure consent – by users or Websites – and comply with the Consent Decree or privacy laws.

VII. Tolling of the Statute of Limitations

142. Any applicable statutes of limitations have been tolled under (1) the fraudulent concealment doctrine, based on Google's knowing and active concealment and denial of the facts alleged herein and (2) the delayed discovery doctrine, as Plaintiffs did not and could not reasonably have discovered Google's conduct alleged herein until shortly before the Complaint was filed.

143. Throughout the Class Period, Google repeatedly and falsely represented that its users (including Plaintiffs and Class members) could prevent Google from tracking users and collecting their information, such as by using a browser in "private browsing mode."

144. Google never disclosed that it would continue to track users and collect their data

once these steps were performed, nor did Google ever admit that it would still attempt to collect, aggregate, and analyze user data so that it can continue to track individual users even when the user has followed Google's instructions on how to browse privately.

145. Google also further misled users by indicating that data associated with them would be viewable through their account, but Google did not include the user data at issue in this lawsuit (collected while in a private browser mode) in user accounts. Google's failure to do so during the Class period is part of Google's active deception and concealment.

146. Google has also made the following statements, which (1) misrepresent material facts about Google's interception and use of users' data in Incognito and/or private browsing modes and/or (2) omit to state material facts necessary to make the statements not misleading. Google thereby took affirmative steps to mislead Plaintiffs and other users about the privacy of their data when using private browsing modes like Incognito.

- On September 27, 2016, Google Director of Product Management Unni Narayana published an article in which he wrote that Google was giving users "more control with incognito mode" and stated "Your searches are your business. That's why we've added the ability to search privately with incognito mode in the Google app for iOS. When you have incognito mode turned on in your settings, your search and browsing history will not be saved."[47]
- On September 8, 2017, Google Product Manager Greg Fair posted an article titled "Improving our privacy controls with a new Google Dashboard" in which he touted how Google has "[p]owerful privacy controls that work for you" and emphasizing how users had "control" over their information and tools "for controlling your data across Google."[48]
- On May 25, 2018, Google updated its Privacy Policy to state that users are "in

[47] https://blog.google/products/search/the-latest-updates-and-improvements-for/.
[48] https://www.blog.google/topics/safety-security/improving-our-privacy-controls-new-google-dashboard/.

control" and "can also choose to browse the web privately using Chrome in Incognito mode."[49]

- On June 21, 2018, Google Product Manager Jon Hannemann posted an article titled "More transparency and control in your Google Account" in which he wrote: "For years, we've built and refined tools to help you easily understand, protect and control your information. As needs around security and privacy evolve, we will continue to improve these important tools to help you control how Google works for you."[50]
- On May 7, 2019, the New York Times published an opinion piece by Google CEO Sudar Pichai in which he represented that it is "vital for companies to give people clear, individual choices around how their data is used" and that Google focuses on "features that make privacy a reality — for everyone." He specifically referenced Incognito, stating: "For example, we recently brought Incognito mode, the popular feature in Chrome that lets you browse the web without linking any activity to you, to YouTube." He continued: "To make privacy real, we give you clear, meaningful choices around your data."[51]
- On May 7, 2019, during Google's annual I/O conference, Google CEO Sundar Pichai represented that Google's products are "built on a foundation of user trust and privacy" and ensuring "that people have clear, meaningful choices around their data." He specifically referenced Incognito mode in Chrome, stating that Google was bringing Incognito mode to Google Maps: "While in Incognito in Maps, your activity, like the places you search and navigate to, won't be linked to your account."[52]

---

[49] https://policies.google.com/privacy/archive/20171218-20180525?hl=en-US.
[50] https://blog.google/technology/safety-security/more-transparency-and-control-your-google-account/.
[51] https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html.
[52] https://singjupost.com/sundar-pichai-at-google-i-o-2019-keynote-full-transcript/?singlepage=1.

- On October 2, 2019, Google Director of Product Management, Privacy and Data Protection Office Eric Miraglia published an article titled "Keeping privacy and security simple, for you" in which he touted Google's decision to add Incognito mode to Google Maps, stating: "When you turn on Incognito mode in Maps, your Maps activity on that device, like the places you search for, won't be saved to your Google Account and won't be used to personalize your Maps experience."[53]
- On December 19, 2019, Google Vice President of Product Privacy Rahul Roy-Chowdhury published an article titled "Putting you in control: our work in privacy this year" in which he noted that Google had "expanded incognito mode across all our apps" as an example of Google's "tools to give you control over your data."[54]
- On January 28, 2020, Google Vice President of Product Privacy Rahul Roy-Chowdhury published an article titled "Data Privacy Day: seven ways we protect your privacy" in which he identified Incognito mode as one of the ways Google keeps "you in control of your privacy" and touted how "Incognito mode has been one of our most popular privacy controls since it launched with Chrome in 2008."[55]
- On or about July 29, 2020, Google submitted written remarks to Congress for testimony by its current CEO Sundar Pichai (who helped develop Google's Chrome browser), which stated: "I've always believed that privacy is a universal right and should be available to everyone and Google is committed to keeping your information safe, treating it responsibly and putting you in control of what you choose to share."[56]

147. The above Google representations were false. Google did not provide users with

---

[53] https://blog.google/technology/safety-security/keeping-privacy-and-security-simple-you/.
[54] https://blog.google/technology/safety-security/putting-you-in-control-privacy-2019/.
[55] https://blog.google/technology/safety-security/data-privacy-day-seven-ways-we-protect-your-privacy/.
[56] https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-PichaiS-20200729.pdf.

control and permit them to browse privately, and Google instead continued to intercept users' communications and collect user data while users were in a private browsing mode such as Incognito. These Google representations, at a minimum, omitted material facts that would be necessary to make the statements made not misleading, as they left the false impression that Google did not intercept and collect users' data while they were in private browsing mode.

148. Moreover, Google's labeling of the relevant products "Incognito" mode and "private browsing" is, in and of itself, misleading absent clear disclosures about the ways in which Google intercepts and uses users' private data. Indeed, "incognito" is defined as "with one's identity concealed." Private is defined as "not known or intended to be known publicly: secret." However, as alleged above, Google in fact intercepts users' private data and then associates that data with the user's "Google profile" across its services—hardly "private" or "Incognito" at all.

149. Plaintiffs relied upon Google's false and misleading representations and omissions that they controlled use of their data through private browsing modes such as Incognito and, based on those misrepresentations, believed that Google was not intercepting and using their private data when they were in such private browsing modes.

150. Plaintiffs did not discover and could not reasonably have discovered, that Google was instead intercepting and using their data in the ways set forth in this Complaint until shortly before the lawsuit was filed in consultation with counsel.

151. Indeed, even after this lawsuit was filed, Google made yet another misleading public statement about its data interception and collection practices. Google spokesperson Jose Castaneda was quoted in articles published in June 2020 stating: "Incognito mode in Chrome gives you the choice to browse the internet without your activity being saved to your browser or device. As we clearly state each time you open a new incognito tab, websites might be able to collect information about your browsing activity during your session." Once again, Google left the misleading impression that users' data was not being intercepted and collected without their knowledge and omitted to disclose the ways in which Google actually intercepts and uses user data in private browsing sessions.

152. Plaintiffs exercised reasonable diligence to protect their data from interception.

Indeed, that is precisely the reason *why* they used Google's "Incognito" and private browsing modes. Yet they did not and could not reasonably have discovered their claims until consulting with counsel shortly before the filing of this Complaint through the exercise of reasonable diligence.

153. Accordingly, Plaintiffs and the Class could not have reasonably discovered the truth about Google's practices until shortly before this class litigation was commenced. Plaintiffs only learned of the truth in the weeks leading up to the filing of this Complaint.

VIII. Google Collected the Data for the Purpose of Committing Further Tortious and Unlawful Acts

154. Google collected the data from users in "private browsing mode" for the purpose of committing additional tortious and unlawful acts. Google's subsequent use of the data violated the California Consumer Privacy Act (CCPA) and the FTC's 2011 Consent Decree. Google also used the data to tortiously invade consumers' privacy and intrude on their seclusion.

155. ***Google collected the data with the intent to violate the California Consumer Privacy Act (CCPA).*** The data collected from users in "private browsing mode" qualifies as "personal information" that is protected by the CCPA. Cal. Civ. Code § 1798.140(o).

The CCPA provides:

> "A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not . . . use personal information collected for additional purposes without providing the consumer with notice consistent with this section."

Cal. Civ. Code § 1798.100(b) (emphasis added).

156. At the time Google collected data from users in "private browsing mode," Google intended to "use" that data "for additional purposes without providing the consumer with notice consistent with this section." Whenever Google uses the confidential communications wrongfully collected, or aggregates it with other information to gain additional insight and intelligence, Google has violated the express prohibitions of the CCPA.

157. Moreover, Google carried out its intent: As described elsewhere in this complaint,

Google made use of the data it collected from users in "private browsing mode," for "additional purposes." The users had never been "informed" of those "additional purposes." Google never gave its users "notice consistent with" the CCPA's requirements regarding these "additional purposes" for which Google used the data collected from users in "private browsing mode."

158. ***Google collected the data with the intent to violate the FTC's 2011 Consent Decree.*** The FTC ordered Google to obtain "express affirmative consent" from each user, "prior to any new or additional sharing" of a user's information that is "a change from stated sharing practices in effect at the time [Google] collected such information."[57]

159. At the time Google collected data from users in "private browsing mode," Google intended to share that data with third parties, in a manner that was very different from the "stated sharing practices" Google had disclosed to users. Google intended to do this without obtaining consent from the users.

160. Moreover, Google carried out its intent: Google shared and/or sold the data, collected from users in "private browsing mode," with third-parties including Google's advertising customers. That sharing and/or selling of data contradicted Google's repeated assurances to users, described herein. Google shared this data without obtaining consent.

161. ***Google collected the data with the intent to intrude upon users' seclusion and invade their constitutional privacy.*** The California Constitution and common law protect consumers from invasions of their privacy and intrusion upon seclusion.

162. Users of the Internet enable "private browsing mode" for the purpose of preventing others—including others in their own household, with whom they share devices—from finding out what the users are viewing on the Internet. For example, users' Internet activity, while in "private browsing mode," may reveal: a user's dating activity; a user's sexual interests and/or orientation; a user's political or religious views; a user's travel plans; a user's private plans for the future (e.g., purchasing of an engagement ring). These are just a few of the many intentions, desires, plans, and

---

[57] *In the Matter of Google, Inc.*, No. C-4336, Decision and Order Part II, p.3 (F.T.C. Oct. 13, 2011), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter.

activities that users intend to keep private when they enable "private browsing mode."

163. It is common knowledge that Google collects information about the web-browsing activity of users who are not in "private browsing mode." It is also common knowledge that Google causes targeted advertisements to be sent based on that information. For example, a reasonable person who (a) uses a shared laptop computer to access a website (e.g., the L.A. Times) and who (b) sees displayed on that website a targeted advertisement for a wedding engagement ring; would therefore (c) believe that some other user of the shared computer had, while not in "private browsing mode," viewed content relating to engagement rings.

164. By causing targeted advertisements to be sent to users and to users' devices, based on data collected while users were in "private browsing mode," Google has caused that data to be revealed to others and has thereby invaded the privacy and intruded upon the seclusion, of the users whose data was collected while in "private browsing mode."

165. Google had the intent to send these targeted advertisements at the time that Google was collecting data from users who were in "private browsing mode."

FACTUAL ALLEGATIONS REGARDING THE NAMED PLAINTIFFS

166. Plaintiff Brown is an adult domiciled in California and has an active Google account and had an active account during the entire Class Period.

167. He accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices.

168. Since at least 2016, Mr. Brown has been a user of various Google products, including Google Maps, Waze, Gmail, and the Chrome browser. At various times since 2016, including between February 28 and May 31, 2020, Mr. Brown visited several major websites using Chrome, in Incognito mode, on his Android devices, which included Android mobile phones and laptops. These websites included but are not limited to Apartments.com, CNN.com, and *latimes.com*, and other private websites. Although Mr. Brown did not know at that time, Plaintiffs are informed and believe now that Google was still tracking Mr. Brown, via various Android and Google-branded software and services, in addition to the X-client-Data Header.

169. Google thereby tracked Mr. Brown and intercepted his communications with Websites. Many of these requests were URL requests that revealed what he viewed and when.

170. Mr. Brown is aware that he is able to sell his own personal data, via other websites such as Killi (https://killi.io/earn/). Unlike these other websites that ask for Mr. Brown's permission to sell his data in exchange for consideration, Google never asked for his permission and instead impermissibly intercepts his communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Mr. Brown's privacy and his ability to control his own personal rights and data.

171. Plaintiff Nguyen is an adult domiciled in California and has an active Google account and had an active account during the entire proposed Class Period.

172. She accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices.

173. Since at least 2016, Ms. Nguyen has been a user of various Google products, including Google Maps, Waze, Gmail, and the Chrome browser. At various times since 2016, including between February 28 and May 31, 2020, Ms. Nguyen visited several major websites using Chrome, in Incognito mode, on her Apple devices, which included her iPhone and MacBook. She also visited several major websites using Safari, in private mode, on her Apple devices. These Websites included various major shopping sites and online publishers of fashion and Google is in possession of a full record of these Websites. Although Ms. Nguyen did not know at that time, Plaintiffs are informed and believe now that Google was still tracking Ms. Nguyen, via various Google-branded software and services.

174. However, Google thereby tracked Ms. Nguyen and intercepted her communications with Websites. Many of these requests were URL requests that revealed what she viewed and when.

175. Ms. Nguyen is aware that she is able to sell her own personal data, via other websites such as Killi (https://killi.io/earn/). Unlike these other websites that ask for Ms. Nguyen's permission to sell her data in exchange for consideration, Google never asked for her permission and instead impermissibly intercepts her communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Ms. Nguyen's privacy

and her ability to control her own personal rights and data.

176. Plaintiff Byatt is an adult domiciled in Florida and has an active Google account and had an active account during the entire proposed Class Period.

177. He accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices.

178. Since at least 2016, Mr. Byatt has been a user of various Google products, including Google Maps, Waze, Gmail, and the Chrome browser. At various times since 2016, including between February 28 and May 31, 2020, Mr. Byatt visited several major websites using Chrome, in Incognito mode, on his Android and Apple devices, which included Android mobile phones. These Websites included, *The New York Times* (nytimes.com) and *The Washington Post* (Washingtonpost.com), and other private websites, and Google is in possession of a full record of these Websites. Although Mr. Byatt did not know at that time, Plaintiffs are informed and believe now that Google was still tracking Mr. Byatt, via various Android and Google-branded software and services, in addition to the X-client-Data Header.

179. Google thereby tracked Mr. Byatt and intercepted his communications with Websites. Many of these requests were URL requests that revealed what he viewed and when.

180. Mr. Byatt is aware that he is able to sell his own personal data, via other websites such as Killi (https://killi.io/earn/). Unlike these other websites that ask for Mr. Byatt's permission to sell his data in exchange for consideration, Google never asked for his permission and instead impermissibly intercepts his communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Mr. Byatt's privacy and his ability to control his own personal rights and data.

181. Plaintiff Davis is an adult domiciled in Arkansas and has an active Google account and had an active account during the entire proposed Class Period.

182. He accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices.

183. Since at least 2016, Mr. Davis has been a user of various Google products, including Google Maps, Gmail, and the Chrome browser. At various times since 2016, including between

February 28 and May 31, 2020, Mr. Davis visited several major websites using Chrome, in Incognito mode, on his laptops and Apple device, which included his Apple iPhone. These Websites included various news organizations' sites, crypto-currency sites, and other private websites, and Google is in possession of a full record of these Websites. Although Mr. Davis did not know at the that time, Plaintiffs are informed and believe now that Google was still tracking Mr. Davis, via various Google-branded software and services, in addition to the X-client-Data Header.

184. Google thereby tracked Mr. Davis and intercepted his communications with Websites. Many of these requests were URL requests that revealed what he viewed and when.

185. Mr. Davis is aware that he is able to sell his own personal data, via other websites such as Killi (https://killi.io/earn/). Unlike these other websites that ask for Mr. Davis' permission to sell his data in exchange for consideration, Google never asked for his permission and instead impermissibly intercepts his communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Mr. Davis' privacy and his ability to control his own personal rights and data.

186. Plaintiff Castillo is an adult domiciled in California and has an active Google account and had an active account during the entire proposed Class Period.

187. He accessed the internet and sent and received communications with Websites on several computing devices that were not shared devices.

188. Since at least 2016, Mr. Castillo has been a user of various Google products, including Google Maps, Gmail, and the Chrome browser. At various times since 2016, including between February 28 and May 31, 2020, Mr. Castillo visited several major websites using Chrome, in Incognito mode, on his laptop and Android device, which included his Android-based Samsung phone. These Websites included dating websites and other private websites, and Google is in possession of a full record of these Websites. Although Mr. Castillo did not know at that time, Plaintiffs are informed and believe now that Google was still tracking Mr. Castillo, via various Android and Google-branded software and services, in addition to the X-client-Data Header.

189. Google thereby tracked Mr. Castillo and intercepted his communications with

Websites. Many of these requests were URL requests that revealed what he viewed and when.

190. Mr. Castillo is aware that he is able to sell his own personal data, via other websites such as Killi (https://killi.io/earn/). Unlike these other websites that ask for Mr. Castillo's permission to sell his data in exchange for consideration, Google never asked for his permission and instead impermissibly intercepts his communications with Websites, and sells information gleaned from such communications. Google's practices irreparably damage Mr. Castillo's privacy and his ability to control his own personal rights and data.

191. None of these Plaintiffs consented to the tracking and interception of their confidential communications made while browsing in "private browsing mode."

CLASS ACTION ALLEGATIONS

192. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of the following Classes:

- Class 1 – All Android device owners who accessed a website containing Google Analytics or Ad Manager using such a device and who were (a) in "private browsing mode" on that device's browser and (b) were not logged into their Google account on that device's browser, but whose communications, including identifying information and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present (the "Class Period").

- Class 2 – All individuals with a Google account who accessed a website containing Google Analytics or Ad Manager using any non-Android device and who were (a) in "private browsing mode" in that device's browser, and (b) were not logged into their Google account on that device's browser, but whose communications, including identifying information and online browsing history, Google nevertheless intercepted, received, or collected from June 1, 2016 through the present (the "Class Period").

193. Excluded from the Classes are: (1) the Court (including any Judge or Magistrate presiding over this action and any members of their families); (2) Defendant, its subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of them have a controlling interest and its officers, directors, employees, affiliates, legal representatives;

(3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel, Class counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

194. **Ascertainability**: Membership of the Classes is defined based on objective criteria and individual members will be identifiable from Google's records, including from Google's massive data storage, consumer accounts, and enterprise services. Based on information readily accessible to it, Google can identify members of the Classes who own an Android device or have a non-Android device with an associated Google account, who were victims of Google's impermissible interception, receipt, or tracking of communications as alleged herein.

195. **Numerosity**: Each of the Classes likely consists of millions of individuals. Accordingly, members of the Classes are so numerous that joinder of all members is impracticable. Class members may be identified from Defendant's records, including from Google's consumer accounts and enterprise services.

196. **Predominant Common Questions**: Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Common questions for the Classes include, but are not limited to, the following:

a. Whether Google represented that Class Members could control what communications of user information, browsing history and web activity data were intercepted, received, or collected by Google;

b. Whether Google gave the Class members a reasonable expectation of privacy that their communications of user information, browsing history and web activity data were not being intercepted, received, or collected by Google when the Class member was using a browser while in "private browsing mode";

c. Whether Google in fact intercepted, received, or collected communications of user information, browsing history and web activity from Class members when the Class members were using a browser while in "private browsing

mode";

d. Whether Google's practice of intercepting, receiving, or collecting communications of user information, browsing history and web activity violated state and federal privacy laws;

e. Whether Google's practice of intercepting, receiving, or collecting communications of user information, browsing history and web activity violated state and federal anti-wiretapping laws;

f. Whether Google's practice of intercepting, receiving, or collecting communications of user information, browsing history and web activity violated any other state and federal tort laws;

g. Whether Plaintiffs and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

h. Whether Plaintiffs and Class members have sustained damages as a result of Google's conduct and if so, what is the appropriate measure of damages or restitution.

197. **Typicality**: Plaintiffs' claims are typical of the claims of other Class members, as all members of the Classes were uniformly affected by Google's wrongful conduct in violation of federal and state law as complained of herein.

198. **Adequacy of Representation**: Plaintiffs will fairly and adequately protect the interests of the members of the Classes and have retained counsel that is competent and experienced in class action litigation, including nationwide class actions and privacy violations. Plaintiffs and their counsel have no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class members. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so.

199. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. This proposed class action presents fewer management difficulties than individual litigation and provides the benefits of a single adjudication, economies of scale and comprehensive supervision by a single, able court.

Furthermore, as the damages individual Class members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

200. **California Law Applies to the Entirety of Both Classes**: California's substantive laws apply to every member of the Classes, regardless of where in the United States the Class member resides, or to which Class the Class member belongs. Defendant's own Terms of Service explicitly states "California law will govern all disputes arising out of or relating to these terms, service specific additional terms, or any related services, regardless of conflict of laws rules. These disputes will be resolved exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts." By choosing California law for the resolution of disputes covered by its Terms of Service, Google concedes that it is appropriate for this Court to apply California law to the instant dispute to all Class members. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs and the Class members under the Due Process Clause, *see* U.S. CONST. amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. CONST. art. IV, § 1, of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by the Plaintiffs and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair. Defendant's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible. The application of California laws to the Classes is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and the proposed Classes and California has the greatest interest in applying its laws here.

201. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

COUNTS

COUNT ONE: VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. § 2510, *ET. SEQ.*

202. Plaintiffs hereby incorporate Paragraphs 1 through 201 as if fully stated herein.

203. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

204. The Wiretap Act protects both the sending and receipt of communications.

205. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

206. Google's actions in intercepting and tracking user communications while they were browsing the internet using a browser while in "private browsing mode" was intentional. On information and belief, Google is aware that it is intercepting communications in these circumstances and has taken no remedial action.

207. Google's interception of internet communications that the Plaintiffs and Class members were sending and receiving while browsing the internet using a browser while in "private browsing mode" was done contemporaneously with the Plaintiffs' and Class members' sending and receipt of those communications.

208. The communications intercepted by Google included "contents" of electronic communications made from the Plaintiffs and Class members to Websites other than Google in the form of detailed URL requests, webpage browsing histories and search queries which Plaintiffs sent to those websites and for which Plaintiffs received communications in return from those websites.

209. The transmission of data between Plaintiffs and Class members on the one hand and the websites on which Google tracked and intercepted their communications on the other, without authorization while they were in "private browsing mode" were "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

210. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The computer codes and programs Google used to track the Plaintiffs' and Class members' communications while they were in "private browsing

mode";

b. The Plaintiffs' and Class members' browsers and mobile applications;

c. The Plaintiffs' and Class members' computing and mobile devices;

d. Google's web and ad servers;

e. The web and ad-servers of websites from which Google tracked and intercepted the Plaintiffs' and Class members' communications while they were using a web browser in "private browsing mode";

f. The computer codes and programs used by Google to effectuate its tracking and interception of the Plaintiffs' and Class members' communications while using a web browser while in "private browsing mode"; and

g. The plan Google carried out to effectuate its tracking and interception of the Plaintiffs' and Class members' communications while using a web browser while in "private browsing mode."

211. Google, in its conduct alleged here, was not providing an "electronic communication service," as that term is defined in 18 U.S.C. § 2510(12) and is used elsewhere in the Wiretap Act. Google was not acting as an Internet Service Provider (ISP). The conduct alleged here does not arise from Google's separate Gmail business of email communications or Google's separate GChat business of instant messages.

212. Google was not an authorized party to the communication because the Plaintiffs and Class members were unaware of Google's redirecting of the referer URLs and webpage browsing histories to Google itself, did not knowingly send any communication to Google, were browsing the internet using a browser while in "private browsing mode," when Google intercepted the communications between the Plaintiffs and websites other than Google. Google could not manufacture its own status as a party to the Plaintiffs' and Class members' communications with others by surreptitiously redirecting or intercepting those communications.

213. As illustrated herein, the communications between the Plaintiffs and Class members on the one hand, and websites on the other, were simultaneous to, but *separate* from, the channel

through which Google acquired the contents of those communications.

214. The Plaintiffs and Class members did not consent to Google's continued gathering of the user's communications after enabling "private browsing mode on their web browser," and thus never consented to Google's interception of their communications. Indeed, Google represented to Plaintiffs, Class members and the public at large that users could "control . . . what information [they] share with Google" and "browse the web privately" by browsing in "private browsing mode." Moreover, the communications intercepted by Google were plainly confidential, which is evidenced by the fact that Plaintiffs and Class members enabled "private browsing mode" in a manner consistent with Google's own recommendations to prevent sharing of information with Google prior to accessing or communicating with the referer URLs and webpage browsing histories.

215. Websites never consented to Google's gathering of the user's communications after enabling private browsing mode on their web browser. The interception by Google in the aforementioned circumstances were unlawful and tortious.

216. After intercepting the communications, Google then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

217. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs and Class members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Google in the future, and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT TWO: VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), CALIFORNIA PENAL CODE §§ 631 AND 632

218. Plaintiffs hereby incorporate Paragraphs 1 through 201 as if fully stated herein.

219. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and

> techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

220. California Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . .

221. California Penal Code § 632(a) provides, in pertinent part:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars . . . .

222. Under either section of the CIPA, a defendant must show it had the consent of all parties to a communication.

223. Google has its principal place of business in California; designed, contrived and effectuated its scheme to track its users while they were browsing the internet from a browser while in "private browsing mode"; and has adopted California substantive law to govern its relationship with its users.

224. At all relevant times, Google's tracking and interceptions of the Plaintiffs' and Class members' internet communications while using a browser in "private browsing mode" was without authorization and consent from the Plaintiffs (and Class members) or Websites. The interception

by Google in the aforementioned circumstances were unlawful and tortious.

225. Google's non-consensual tracking of the Plaintiffs' and Class members' internet communications who were on their web browser or using a browser in "private browsing mode" was designed to attempt to learn at least some meaning of the content in the URLs.

226. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Google's deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. The computer codes and programs Google used to track the Plaintiffs' and Class members' communications while they were in "private browsing mode";

b. The Plaintiffs' and Class members' browsers and mobile applications;

c. The Plaintiffs' and Class members' computing and mobile devices;

d. Google's web and ad servers;

e. The web and ad-servers of websites from which Google tracked and intercepted the Plaintiffs' and Class members' communications while they were using a web browser in "private browsing mode";

f. The computer codes and programs used by Google to effectuate its tracking and interception of the Plaintiffs' and Class members' communications while using a web browser in "private browsing mode"; and

g. The plan Google carried out to effectuate its tracking and interception of the Plaintiffs' and Class members' communications while using a browser in "private browsing mode."

227. The data collected by Google constituted "confidential communications," as that term is used in Section 632, because Plaintiffs and Class members had objectively reasonable expectations of privacy while browsing in "private browser mode."

228. Plaintiffs and Class members have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally-

identifiable information.

229. Pursuant to California Penal Code § 637.2, Plaintiffs and Class members have been injured by the violations of California Penal Code §§ 631 and 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT THREE: VIOLATIONS OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE § 502 *ET SEQ.*

230. Plaintiffs hereby incorporate Paragraphs 1 through 201 as if fully stated herein.

231. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction." Smart phone devices with the capability of using web browsers are "computers" within the meaning of the statute.

232. Google violated Cal. Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, analyzing, and using Plaintiffs' and Class members' data.

233. Despite Google's false representations to the contrary, Google effectively charged Plaintiffs, Class Members, and other consumers and Google was unjustly enriched, by acquiring their sensitive and valuable personal information without permission and using it for Google's own financial benefit to advance its advertising business. Plaintiffs and Class members retain a stake in the profits Google earned from their personal browsing histories and other data because, under the circumstances, it is unjust for Google to retain those profits

234. Google accessed, copied, took, analyzed, and used data from Plaintiffs' and Class members' computers in and from the State of California, where Google: (1) has its principal place of business; and (2) used servers that provided communication links between Plaintiffs' and Class members' computers and Google, which allowed Google to access and obtain Plaintiffs' and Class members' data. Accordingly, Google caused the access of Plaintiffs' and Class members' computers from California, and is therefore deemed to have accessed Plaintiffs' and Class members' computers in California.

235. As a direct and proximate result of Google's unlawful conduct within the meaning

of Cal. Penal Code § 502, Google has caused loss to Plaintiffs and Class members and has been unjustly enriched in an amount to be proven at trial.

236. Plaintiffs, on behalf of themselves and Class members, seek compensatory damages and/or disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

237. Plaintiffs and Class members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Google's violations were willful and, upon information and belief, Google is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

238. Plaintiffs and the Class members are also entitled to recover their reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

COUNT FOUR: INVASION OF PRIVACY

239. Plaintiffs hereby incorporate Paragraphs 1 through 238 as if fully stated herein.

240. The right to privacy in California's constitution creates a right of action against private entities such as Google.

241. Plaintiffs' and Class members' expectation of privacy is deeply enshrined in California's Constitution**.** Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted by California voters in 1972.

242. The phrase "and privacy" was added in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating:

> The right of privacy is the right to be left alone…It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control

> circulation of personal information. This is essential to social relationships and personal freedom.[58]

243. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Google.

244. To plead a California constitutional privacy claim, a plaintiff must show an invasion of (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

245. As described herein, Google has intruded upon the following legally protected privacy interests:

a. The Federal Wiretap Act as alleged herein;

b. The California Wiretap Act as alleged herein;

c. A Fourth Amendment right to privacy contained on personal computing devices, including web-browsing history, as explained by the United States Supreme Court in the unanimous decision of *Riley v. California*;

d. The California Constitution, which guarantees Californians the right to privacy;

e. Google's Privacy Policy and policies referenced therein and other public promises it made not to track or intercept the Plaintiffs' and Class members' communications or access their computing devices and web-browsers while browsing in "private browsing mode."

246. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances in that Plaintiffs and Class members could not reasonably expect Google would commit acts in violation of federal and state civil and criminal laws; and Google affirmatively promised users (including Plaintiffs and Class members) it would not track their communications or access their computing devices or web-browsers while they were using a web browser while in

---

[58] BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH ARGUMENTS TO VOTERS, GEN. ELECTION *26 (Nov. 7, 1972).

"private browsing mode."

247. Google's actions constituted a serious invasion of privacy in that it:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including web search and browsing histories;

b. Violated several federal criminal laws, including the Wiretap Act;

c. Violated dozens of state criminal laws on wiretapping and invasion of privacy, including the California Invasion of Privacy Act;

d. Invaded the privacy rights of hundreds of millions of Americans (including Plaintiffs and class members) without their consent;

e. Constituted the unauthorized taking of valuable information from hundreds of millions of Americans through deceit; and

f. Further violated Plaintiffs' and Class members' reasonable expectation of privacy via Google's review, analysis, and subsequent uses of Plaintiffs' and Class members' private and other browsing activity that Plaintiffs and Class members considered sensitive and confidential.

248. Committing criminal acts against hundreds of millions of Americans constitutes an egregious breach of social norms that is highly offensive.

249. The surreptitious and unauthorized tracking of the internet communications of millions of Americans, particularly where, as here, they have taken active (and recommended) measures to ensure their privacy, constitutes an egregious breach of social norms that is highly offensive.

250. Google's intentional intrusion into Plaintiffs' and Class members' internet communications and their computing devices and web-browsers was highly offensive to a reasonable person in that Google violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

251. The taking of personally-identifiable information from hundreds of millions of Americans through deceit is highly offensive behavior.

252. Secret monitoring of web private browsing is highly offensive behavior.

253. Following Google's unauthorized interception of the sensitive and valuable personal information, the subsequent analysis and use of that private browsing activity to develop and refine profiles on Plaintiffs, Class members, and consumers violated their reasonable expectations of privacy.

254. Wiretapping and surreptitious recording of communications is highly offensive behavior.

255. Google lacked a legitimate business interest in tracking users while browsing the internet on a browser while in "private browsing mode," without their consent.

256. Plaintiffs and Class members have been damaged by Google's invasion of their privacy and are entitled to just compensation and injunctive relief.

COUNT FIVE: INTRUSION UPON SECLUSION

257. Plaintiffs hereby incorporate Paragraphs 1 through 238 as if fully stated herein.

258. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

259. In carrying out its scheme to track and intercept Plaintiffs' and Class members' communications while they were using a browser while in "private browsing mode" in violation of its own privacy promises, Google intentionally intruded upon the Plaintiffs' and Class members' solitude or seclusion in that it effectively placed itself in the middle of conversations to which it was not an authorized party.

260. Google's tracking and interception were not authorized by the Plaintiffs and Class members, the Websites with which they were communicating, or even the Plaintiffs' and Class members' web-browsers.

261. Google's intentional intrusion into their internet communications and their computing devices and web-browsers was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

262. The taking of personally-identifiable information from hundreds of millions of Americans through deceit is highly offensive behavior, particularly where, as here, Plaintiffs and Class members took active (and recommended) measures to ensure their privacy.

263. Secret monitoring of web private browsing is highly offensive behavior.

264. Wiretapping and surreptitious recording of communications is highly offensive behavior.

265. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person is browsing the internet in "private browsing mode."

266. Plaintiffs and the Class members have been damaged by Google's invasion of their privacy and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Appoint Plaintiffs to represent the Classes;

C. Appoint undersigned counsel to represent the Classes;

D. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

E. Award nominal damages to Plaintiffs and the Class members against Defendant;

F. Ordering Defendant to disgorge revenues and profits wrongfully obtained;

G. Permanently restrain Defendant, and its officers, agents, servants, employees and attorneys, from intercepting, tracking, or collecting communications after class members used a browser while in "private browsing mode," or otherwise violating its policies with users;

H. Award Plaintiffs and the Class members their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

I. Grant Plaintiffs and the Class members such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

The Plaintiffs demand a trial by jury of all issues so triable.

Dated: September 21, 2020

BOIES SCHILLER FLEXNER LLP

/s/ Mark C. Mao
Mark C. Mao

Mark C. Mao, CA Bar No. 236165
Sean P. Rodriguez, CA Bar No. 262437
Beko Richardson, CA Bar No. 238027
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899
mmao@bsfllp.com
srodriguez@bsfllp.com
brichardson@bsfllp.com

James Lee (admitted *pro hac vice*)
Rossana Baeza (admitted *pro hac vice*)
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
Fax: (303) 539-1307
jlee@bsfllp.com
rbaeza@bsfllp.com

Amanda K. Bonn, CA Bar No. 270891
SUSMAN GODFREY L.L.P
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA. 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
abonn@susmangodfrey.com

William S. Carmody (admitted *pro hac vice*)
Shawn Rabin (admitted *pro hac vice*)
Steven M. Shepard (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019-6023
Tel.: (212) 336-8330
Fax: (212) 336-8340
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com

John A. Yanchunis (admitted *pro hac vice*)
Ryan J. McGee (admitted *pro hac vice*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com

Attorneys for Plaintiffs